UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, AND CIP-011-2

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charles.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

February 13, 2015

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, AND CIP-011-2

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA"),[1] Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] and Order No. 791,[3] the North American Electric Reliability Corporation ("NERC")[4] hereby submits for Commission approval the following proposed Critical Infrastructure Protection ("CIP") Reliability Standards:

- CIP-003-6 – Cyber Security – Security Management Controls
- CIP-004-6 – Cyber Security – Personnel and Training
- CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-6 – Cyber Security – Systems Security Management
- CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-2 – Cyber Security – Information Protection

---

1 16 U.S.C. § 824o (2006).

2 18 C.F.R. § 39.5 (2014).

3 *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and rehearing*, Order No. 791-A, 146 FERC ¶ 61, 188 (2014).

4 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

NERC requests that the Commission approve the proposed Reliability Standards, provided in Exhibit A hereto, as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

NERC also requests approval of:

- the associated Implementation Plan (Exhibit B);
- the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A and E);
- the proposed new or revised definitions to be incorporated into the NERC Glossary of Terms Used in Reliability Standards ("NERC Glossary") for the following terms: (1) BES Cyber Asset, (2) Protected Cyber Asset ("PCA"), (3) Low Impact BES Cyber System Electronic Access Point ("LEAP"), (4) Low Impact External Routable Connectivity ("LERC"); (5) Removable Media, and (6) Transient Cyber Asset (Exhibit A); and
- the retirement of Commission-approved Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1.

As required by Section 39.5(a) of the Commission's regulations,[5] this Petition presents the technical basis and purpose of the proposed Reliability Standards, a summary of the development history (Exhibit F), and a demonstration that the proposed Reliability Standards meet the criteria identified by the Commission in Order No. 672[6] (Exhibit C). The NERC Board of Trustees ("Board") adopted proposed Reliability Standards CIP-006-6 and CIP-009-6 on November 13, 2014 and proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 on February 12, 2015.[7]

---

[5] 18 C.F.R. § 39.5(a) (2013).

[6] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, at P 262, 321-37, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[7] Unless otherwise designated, all capitalized terms used herein shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

I. EXECUTIVE SUMMARY

The purpose of NERC's CIP cybersecurity Reliability Standards is to mitigate the cybersecurity risks to Bulk Electric System Facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cyber-attack, would affect the reliable operation of the Bulk Electric System. On November 22, 2013, the Commission issued Order No. 791, approving new and modified CIP cybersecurity Reliability Standards, collectively referred to as the CIP Version 5 Standards, to become effective on April 1, 2016.[8] As the Commission stated, the CIP Version 5 Standards represent an improvement over the currently-effective CIP Reliability Standards as they adopt new cybersecurity controls and extend the scope of the systems protected by the CIP Reliability Standards.[9] While the Commission approved the CIP Version 5 Standards, it also directed NERC to develop the following modifications to improve those standards:

1. Modify or remove the language in 17 requirements in the CIP Version 5 Standards that requires responsible entities to implement cyber security policies in a manner that "identifies, assesses, and corrects deficiencies."[10]

2. Develop modifications to the CIP Version 5 Standards to address security controls for low impact BES Cyber Systems.[11]

3. Develop requirements that protect transient devices (e.g., thumb drives, laptop computers, and other devices that are portable and frequently connected and disconnected from systems on a temporary basis) that fall outside the definitions for BES Cyber Asset and PCA.[12]

4. Create a definition of "communication networks" and develop new or modified standards that address the protection of the nonprogrammable components of communication networks.[13]

---

[8] The Commission also approved 19 new or revised defined terms used in the CIP Version 5 Standards for incorporation into the NERC Glossary.

[9] Order No. 791 at PP 1-2; 41.

[10] *Id*. at PP 4, 67-76.

[11] *Id*. at PP 5, 106-110.

[12] *Id*. at PP 6, 132-136.

[13] *Id*. at PP 7, 148-150.

The Commission directed NERC to submit for Commission approval revised standards addressing the "identify, assess, and correct" and communication networks directives within one year from the effective date of Order No. 791, which is February 3, 2015.[14] On January 13, 2015, the Commission granted NERC a 10-day extension of the February 3, 2015 deadline.[15] The Commission did not provide a deadline for the directives related to low impact BES Cyber Systems and transient devices.

As discussed further below, the proposed Reliability Standards improve the cybersecurity protections required by the CIP Reliability Standards and collectively address the Commission's four directives from Order No. 791 as follows:

"Identify, Assess, and Correct" Language – Consistent with the Commission's directive, NERC has removed the "identify, assess, and correct" language from the 17 requirements in the CIP Version 5 Standards that included such language.[16] NERC is addressing the concerns underlying the "identify, assess, and correct" language outside the text of a Reliability Standard as part of its risk-based Compliance Monitoring and Enforcement Program ("CMEP"). Specifically, in 2012, NERC launched the Reliability Assurance Initiative ("RAI"), a multi-year effort to identify and implement changes to enhance the effectiveness of the ERO's CMEP by establishing a robust, risk-based approach to compliance monitoring and enforcement. Consistent with the fundamental rationale and principles of the "identify, assess, and correct" language, the purpose of RAI was to design and implement a risk-based CMEP that, among other things: (1) focuses on

[14] Order No. 791 was published in the Federal Register on December 3, 2013 and became effective on February 3, 2014.

[15] *Notice Granting Extension of Time*, Docket No. RM13-5-000 (Jan. 13, 2015).

[16] Those 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5.1, Requirements R2, R3, R4, and R5; CIP-006-5, Requirements R1 and R2; CIP-007-5, Requirements R1, R2, R3, R4, and R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

improving entities' internal controls; (2) scopes compliance monitoring activities based on risk assessments; (3) provides appropriate deterrence through enforcement; and (4) establishes a feedback loop to improve the content of the Reliability Standards. As discussed in NERC's informational filing in Docket No. RR15-2-000, through RAI, NERC developed a risk-based CMEP that includes processes and programs, such as risk assessments, compliance exceptions, and self-logging of minimal risk issues, that directly accomplish the goals of the "identify, assess, and correct" language.[17] In 2015, NERC began to implement these new risk-based processes and programs for all registered entities.

Security Controls for Assets Containing Low Impact BES Cyber Systems – In response to the Commission's concern that the CIP Version 5 Standards do not contain specific controls for low impact BES Cyber Systems or objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities for their low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6, Requirement R2 requires responsible entities to implement cybersecurity plans for assets containing low impact BES Cyber Systems to meet specific security objectives related to: (i) cybersecurity awareness; (ii) physical security controls; (iii) electronic access controls; and (iv) Cyber Security Incident response. Considering the large number and wide variety of types of low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6 provides responsible entities the flexibility to implement security controls in the manner that best suits the needs and characteristics of their organization. By articulating clear security objectives for each of the four subject matter areas listed above, however, the ERO and

[17] *See* Informational Filing of the North American Electric Reliability Corporation, Docket No. RR15-2-000 (November 3, 2014) (the "RAI Informational Filing).

the Commission will have a basis from which to judge the sufficiency of the controls ultimately adopted by a responsible entity.

Additionally, proposed Reliability Standard CIP-003-6, Requirement R1 requires responsible entities to document cybersecurity policies for their assets containing low impact BES Cyber Systems and for the policies to be reviewed and approved by the CIP Senior Manager. The policies must cover the same four areas as the Requirement R2 plans: cybersecurity awareness; physical security controls; electronic access controls; and Cyber Security Incident response. These policies, like the policies already required for high and medium impact BES Cyber Systems, will communicate the responsible entity's management goals, objectives, and expectations for the protection of low impact BES Cyber Systems. These policies will help establish an overall governance foundation for creating a culture of security and compliance.

Protection of Transient Devices – As the Commission recognized in Order No. 791, transient devices are potential vehicles for cyber-attacks absent appropriate controls.[18] To improve the defense-in-depth approach of the CIP Reliability Standards, the proposed Reliability Standards include specific requirements applicable to transient devices to further mitigate the security risks associated with such devices. Specifically, proposed Reliability Standard CIP-010-2, Requirement R4 requires entities to implement controls to protect transient devices connected to their high impact and medium impact BES Cyber Systems and associated PCAs. Responsible entities must implement controls to accomplish the following security objectives:

- prevent unauthorized access to and use of transient devices;
- mitigate the risk of vulnerabilities associated with unpatched software on transient devices; and

[18] Order No. 791 at PP 134-135.

- mitigate the risk of the introduction of malicious code on transient devices.

Similar to the framework established for protecting low impact BES Cyber Systems, responsible entities have the flexibility to determine the controls necessary to meet these security objectives. By articulating the clear security objectives described above, however, the ERO and the Commission will have a basis from which to judge the sufficiency of the controls ultimately adopted by a responsible entity. Additionally, proposed Reliability Standard CIP-004-6, Requirement R2, Part 2.1 requires entities to provide training on the risks associated with transient devices.

Under the proposed Reliability Standards, transient devices are classified as either "Transient Cyber Assets" or "Removable Media" depending on their functionality. The terms "Transient Cyber Assets" and "Removable Media" are proposed terms for inclusion in the NERC Glossary that define the types of transient devices subject to the CIP Reliability Standards. The term "Transient Cyber Assets" refers to those programmable electronic devices, such as laptops, that are not otherwise included in a BES Cyber System or categorized as PCAs and that are used to connect on a temporary basis (i.e., 30 calendar days or less) to BES Cyber Assets, networks within an Electronic Security Perimeter ("ESP"), or PCAs for purposes such as data transfer, vulnerability assessment, maintenance, or troubleshooting. The term "Removable Media" refers to storage media that are nonprogrammable and used to connect on a temporary basis to BES Cyber Assets, networks within an ESP, or PCAs for purposes such as storing, copying, moving, or accessing data. The requirements applicable to Transient Cyber Assets and Removable Media are tailored to the capabilities of those devices.

Protection of Communication Networks – The proposed Reliability Standards also enhance the protections mandated by the CIP Version 5 Standards by requiring entities to implement security controls for nonprogrammable components of communication networks at

Control Centers with high or medium impact BES Cyber Systems. Specifically, Reliability Standard CIP-006-6, Requirement R1, Part 1.10 requires responsible entities to protect cabling and other nonprogrammable communication components (e.g., unmanaged switches, hubs, patch panels, media converters, port savers, and couplers) that are used to connect applicable Cyber Assets within the same ESP but are located outside of a Physical Security Perimeter ("PSP"). Entities must either (1) restrict physical access to such nonprogrammable communication components, or (2) implement data encryption, circuit monitoring, or equally effective protections. These protections will reduce the likelihood that "man-in-the-middle" attacks could compromise the integrity of BES Cyber Assets or PCAs at Control Centers with high or medium impact BES Cyber Systems.

Additionally, the applicability of proposed Reliability Standard CIP-007-6, Requirement R1, Part 1.2, which requires entities to protect against the use of unnecessary physical input/output ports, now includes PCAs and nonprogrammable communications components associated with high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers. Extending the scope of Part 1.2 to include PCAs and certain nonprogrammable communication components will strengthen the defense-in-depth approach provided by the CIP Reliability Standards by further minimizing the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

For the reasons discussed herein, NERC respectfully requests that the Commission approve the proposed Reliability Standards as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[19]

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Associate General Counsel
Shamai Elstein*
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charles.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Valerie Agnew*
Director of Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
valerie.agnew@nerc.net

III. BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[20] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1) of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards.[21] Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard.[22] Section 39.5(a) of the Commission's regulations requires the ERO to file for Commission approval

[19] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2013), to allow the inclusion of more than two persons on the service list in this proceeding.

[20] 16 U.S.C. § 824o (2006).

[21] *Id.* § 824(b)(1).

[22] *Id.* § 824o(d)(5).

each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.[23]

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.[24]

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standards were developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[25] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[26] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards. The development process is open to any person or entity with a legitimate interest in

---

[23] 18 C.F.R. § 39.5(a) (2012).

[24] 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).

[25] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672 at P 334, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[26] The NERC Rules of Procedure are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders. Further, a vote of stakeholders and adoption by the NERC Board is required before NERC submits the Reliability Standard to the Commission for approval.

C. Development of the Proposed Reliability Standards

As further described in Exhibit F hereto, following the issuance of Order No. 791, NERC initiated a standard development project, Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions ("Project 2014-02"), to address the following directives from Order No. 791: (1) modify or remove the "identify, assess, and correct" language in 17 requirements in the CIP Version 5 Standards; (2) develop modifications to the CIP Version 5 Standards to address security controls for low impact BES Cyber Systems; (3) develop requirements that protect transient devices; and (4) create a definition of "communication networks" and develop new or modified standards that address the protection of nonprogrammable components of communication networks.

In January 2014, the NERC Standards Committee approved a Standard Authorization Request to initiate Project 2014-02 and appointed a standard drafting team. Prior to the first meeting of the standard drafting team, NERC hosted two technical conferences in Atlanta, Georgia (January 21, 2014) and Phoenix, Arizona (January 23, 2014) to discuss the Order No. 791 directives and obtain early feedback from industry participants on possible approaches for revising the CIP Version 5 Standards to respond to the Commission's four directives.

On June 2, 2014, NERC posted the proposed Reliability Standards addressing all four directives for an initial 45-day comment period and ballot. Each of the posted Reliability Standards included revisions to address the "identify, assess, and correct" directive. Proposed Reliability Standards CIP-006-6 and CIP-007-6 also included revisions to address the communication

networks directive, and proposed Reliability Standard CIP-003-6 included revisions to address the low impact directive. The transient devices directive was addressed primarily in proposed Reliability Standard CIP-010-2, but the standard drafting team also made minor revisions in CIP-004-6, CIP-007-6, and CIP-011-2 to address this directive. On initial ballot, proposed Reliability Standards CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-011-2 received the requisite stakeholder approval. The proposed Reliability Standards that primarily addressed the low impact and transient devices directives (CIP-003-6 and CIP-010-2), however, did not receive the requisite stakeholder approval.

The standard drafting team addressed industry comments on the initial drafts of the proposed Reliability Standards, and, on September 3, 2014, NERC posted second drafts of proposed Reliability Standards CIP-003-6 and CIP-010-2 for an additional 45-day comment period and ballot. In addition, to ensure that NERC could satisfy its regulatory deadline, NERC posted for a 45-day comment period and ballot versions of Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 that only addressed the "identify, assess, and correct" and communication networks directives.[27] All of the proposed Reliability Standards received the requisite stakeholder approval on the second posting.

After reviewing industry comment on the second drafts of the proposed Reliability Standards, however, the standard drafting team determined that additional modifications to Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 were necessary to address industry comments on the modifications related to the low impact and transient devices directives. To ensure that it could meet its regulatory deadline, on October 28,

[27] Reliability Standards CIP-006-6 and CIP-009-6 were not posted for an additional ballot because the standards did not previously include any revisions related to the low impact or transient device directives. Further, based on stakeholder comments, the standard drafting team did not identify the need for any further revisions to those standards.

2014, NERC posted for final ballot the versions of the proposed Reliability Standards that only addressed the "identify, assess, and correct" and communication networks directives. These final ballots resulted in the requisite stakeholder approvals (between 83.84% and 95.40%), and the NERC Board adopted these versions of the proposed Reliability Standards on November 13, 2014.

On November 25, 2014, after the standard drafting team addressed industry comment, NERC posted revised versions of proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 for an additional 45-day comment period and ballot to replace the versions of those Reliability Standards adopted by the Board on November 13, 2014. These additional ballots received the requisite stakeholder approval (between 81.92% and 98.89%) and, after receiving the requisite stakeholder approval in final ballots, the Board adopted the revised versions of proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 on February 12, 2015.[28]

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standards satisfy the Commission's criteria in Order No. 672 and are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The following section provides an explanation of the manner in which the proposed Reliability Standards address each of the Order No. 791 directives.

[28] During development, these revised versions of the proposed Reliability Standards were posted as CIP-003-7, CIP-004-7, CIP-007-7, CIP-10-3, and CIP-011-3 to help differentiate the revised versions from the versions adopted by the Board in November 2014. For purposes of Board adoption and filing with applicable governmental authorities, however, the version numbers are presented as -6 and -2 because the versions adopted by the Board in November 2014 were never filed with applicable governmental authorities.

A. Identify, Assess, and Correct Language

i. Order No. 791 Directive

As noted above, there are 17 requirements in the CIP Version 5 Standards that require responsible entities to implement cybersecurity policies or processes in a manner that "identifies, assesses, and corrects deficiencies." The purpose of including the "identify, assess, and correct" language was to move away from a "zero tolerance" compliance and enforcement approach and focus responsible entities on developing strong internal controls to identify and minimize instances of noncompliance. In short, the standard drafting team for the CIP Version 5 Standards recognized that while registered entities should identify, control, and minimize instances of noncompliance with those 17 requirements, it was not reasonable to expect that registered entities will be able to prevent all instances of noncompliance given the breadth and high frequency of the cybersecurity obligations therein. Further, the CIP Version 5 standard drafting team determined that it is possible that individual instances of noncompliance with those 17 requirements would be unlikely to pose a more-than-minimal risk to reliability, particularly where the responsible entity identifies the noncompliance and takes corrective action.

The CIP Version 5 standard drafting team thus concluded that, under these circumstances, the compliance and enforcement process would better promote the goals of reliability through a risk-based model, focusing industry and ERO efforts and resources on improving internal controls and avoiding instances of noncompliance that pose a more-than-minimal risk to reliability. The "identify, assess, and correct" language was intended to recognize the positive benefit to reliability of those responsible entities that have strong cultures of compliance and are proactive in their approach to identify and correct instances of noncompliance.

In Order No. 791, the Commission supported NERC's move away from a "zero tolerance" approach to compliance and the development of standards that encourage entities to improve

internal controls and focus on the activities that have the greatest impact on Bulk-Power System reliability. The Commission expressed concern, however, that the "identify, assess, and correct" language is overly vague and lacking the basic definition and guidance that is needed, for example, to distinguish a successful internal control program from one that is inadequate.[29] As such, the Commission directed NERC to remove or modify that language within one year of the date of Order No. 791. The Commission emphasized its preference for NERC to remove the language from the CIP Version 5 Standards and address the concerns underlying the "identify, assess, correct" language outside of the text of the Reliability Standards.[30] The Commission stated:

> We would prefer approaches that would not involve the placement of compliance language within the text of the Reliability Standards to address these issues. We understand that NERC has inserted the "identify, assess, and correct" language into the CIP Reliability Standard requirements to move its compliance processes towards a more risk-based model. With this objective in mind, we believe that a more appropriate balance might be struck to address the underlying concerns by developing compliance and enforcement processes that would grant NERC and the Regional Entities the ability to decline to pursue low risk violations of the Reliability Standards. Striking this balance could be accomplished through a modification to the Compliance Monitoring and Enforcement Program. We believe that such an approach would: (1) empower NERC and the Regional Entities to implement risk-based compliance monitoring techniques that avoid zero defect enforcement when appropriate; (2) allow the Commission to retain oversight over the enforcement of Reliability Standards; and (3) ensure that all Reliability Standards are drafted to be sufficiently clear and enforceable.[31]

ii. Proposed Modifications

Consistent with Order No. 791, NERC has modified the CIP Version 5 Standards by removing the "identify, assess, and correct" language from the 17 requirements that included such language.[32] NERC is addressing the concerns underlying the inclusion of the "identify, assess,

---

[29] Order No. 791 at PP 4, 67-76.

[30] *Id*. at PP 73-76.

[31] *Id*. at P 75.

[32] Each of the proposed Reliability Standards had at least one requirements with the "identify, assess and correct" language. Specifically, as noted above, the 17 requirements that included such language are: CIP-003-5,

and correct" language outside the text of a Reliability Standard through transformation of its CMEP and the implementation of a risk-based approach to compliance monitoring and enforcement activities.

In 2012, NERC launched RAI, a collaborative effort among NERC, the Regional Entities, and industry to identify and implement changes to enhance the effectiveness of the CMEP. Based on its compliance monitoring and enforcement experience, the ERO determined that a risk-based approach is essential for a proper allocation of ERO and industry resources and encourages registered entities to enhance internal controls, including those regarding the self-identification of potential noncompliance. NERC's experience indicated that a one-size-fits-all and "zero tolerance" approach to compliance monitoring and enforcement does not properly allocate time, attention, and resources to higher-risk instances of noncompliance or demonstrably equate to more reliable operations of the Bulk-Power System. It is not practical, effective, or sustainable to monitor and treat all compliance issues to the same degree or in the same manner regardless of risk and entity management practices.[33] Compliance monitoring and enforcement must be "right-sized" based on a number of considerations, including risk factors and registered entity management practices related to the detection, assessment, mitigation, and reporting of potential noncompliance. To that end, as discussed in greater detail in the RAI Informational Filing, the RAI program involved the testing, through various pilot programs, of a number of concepts,

Requirements R2 and R4; CIP-004-5.1, Requirements R2, R3, R4, and R5; CIP-006-5, Requirements R1 and R2; CIP-007-5, Requirements R1, R2, R3, R4, and R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

[33] For instance, for high frequency security obligations, entities with effective internal controls are likely to find and correct more deficiencies than those entities without a developed approach to compliance. By treating all instances of noncompliance alike, a "zero tolerance" approach would fail to recognize and properly incentivize the development of robust internal control pursuant to which an entity is likely to identify more instances of noncompliance.

processes, and programs to develop a risk-based compliance monitoring and enforcement framework that incentivizes registered entities to develop robust compliance programs.

As a result of RAI, NERC developed a risk-based CMEP that incorporates the fundamental rationale and principles of the "identify, assess, and correct" language.[34] In general, NERC's new approach to compliance monitoring and enforcement:

- Tailors NERC's compliance monitoring and enforcement activities to the risks presented by the registered entity and the risks that the particular Reliability Standard (and/or requirement) under consideration is designed to mitigate;
- Recognizes that not all noncompliance requires formal enforcement action;
- Recognizes and rewards registered entities for efforts to improve internal controls and methods for the prompt self-identification and mitigation of noncompliance;
- Maintains ERO visibility into all instances of noncompliance to identify reliability risks and trends; and
- Maintains ERO oversight to identify implementation issues and opportunities for improvement.

The transformation to a risk-based CMEP involves the use of an oversight plan framework focused on identifying, prioritizing, and addressing risks to the Bulk-Power System to enable each Regional Entity to allocate resources where they are most needed and likely to be the most effective. The result is a compliance oversight plan for each individual registered entity. Specifically, under the risk-based CMEP, Regional Entities conduct inherent risk assessments ("IRAs") for the registered entities within their regions. An IRA is a review of potential risks posed by an individual registered entity to the reliability of the Bulk-Power System. An IRA considers factors such as assets, systems, geography, interconnectivity, and functions performed,

[34] Additional information regarding RAI and NERC's risk-based CMEP is available at http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

among others. The IRAs enable the Regional Entities to tailor oversight appropriately (i.e., focus their compliance monitoring activities on those areas for which the IRA shows greater risk).[35]

Following the IRA, a registered entity may elect to provide the Regional Entity information concerning the internal controls it uses to manage reliability risks. This process, known as the internal control evaluation ("ICE"), allows the Regional Entity to evaluate those internal controls to determine whether a registered entity has implemented effective internal controls that provide reasonable assurance of compliance with Reliability Standards associated with areas of risk identified through the IRA. By understanding how a registered entity manages or mitigates risks, the Regional Entity can further tailor its compliance oversight efforts.

Ultimately, the Regional Entity will determine the type and frequency of the compliance monitoring tools (i.e., off-site or on-site audits, spot checks, or self-certifications) warranted for a particular registered entity based on reliability risks, as determined through the IRA, and information about the registered entity's internal controls learned through the ICE process. The Regional Entity may conduct more resource-intensive compliance monitoring activities with respect to functions or registered entities within its region that can have the most significant impact on reliability. For functional roles or registered entities that have a lesser impact on reliability, the Regional Entity may tailor compliance monitoring approaches accordingly. The IRAs and ICEs thus directly accomplish the goal of the "identify, assess, and correct" language by focusing ERO and industry resources on those areas that pose a more-than-minimal risk to reliability and helping to improve internal controls.

[35] For example, a Regional Entity may choose not to include in the scope of its monitoring activities certain standards or requirements if the IRA shows less risk to reliability for those standards or requirements for that registered entity. Conversely, a Regional Entity may choose to focus its monitoring on areas for which the IRA shows greater risk.

More significantly, the risk-based CMEP also accomplishes the goal of the "identify, assess, and correct" language of moving away from a "zero tolerance" approach by allowing entities to address lower-risk instances of noncompliance outside of a formal enforcement process. Specifically, NERC is implementing (1) a compliance exception program, and (2) a self-logging program. These programs, as discussed in greater detail in the RAI informational filing, leverage existing internal practices at registered entities relating to self-monitoring, identification, assessment, and correction of noncompliance with Reliability Standards. By appropriately valuing and rewarding such efforts (i.e., by providing a disposition path outside of a formal enforcement action), the ERO encourages the enhancement of internal controls and self-identification of noncompliance throughout the industry, consistent with the intent of the "identify, assess, and correct" language. These risk-based programs apply to all Reliability Standards and requirements, not just the 17 CIP Version 5 requirements containing the "identify, assess, and correct" language.

Since 2013, the ERO has exercised discretion when deciding whether to initiate an enforcement action for noncompliance posing a minimal risk to the reliability of the BPS. Issues resolved outside of an enforcement action are referred to as compliance exceptions. Compliance exceptions reflect the "identify, assess, and correct" tenet that not all noncompliance requires processing in a formal enforcement action. Compliance exception treatment is especially appropriate if the registered entity adequately identifies its noncompliance, assesses the risk properly as minimal risk, and corrects (i.e., mitigates) the noncompliance in a timely and appropriate manner. A robust internal compliance program and management practices that led to timely discovery and timely mitigation of noncompliance may support compliance exception treatment. All minimal risk noncompliance, however, is eligible for a compliance exception regardless of discovery method.

Compliance exceptions are similar to issues remediated through the Find, Fix, Track, and Report ("FFT") program in that entities will not incur any financial penalties for issues granted a compliance exception. Compliance exceptions are not subject to formal enforcement processes. Further, a compliance exception is part of a registered entity's compliance history only to the extent that it serves to inform the ERO of potential risk. Compliance exceptions are not part of a registered entity's violation history for purposes of aggravation of penalties. Finally, to maintain visibility and allow for appropriate oversight, all compliance exceptions must be documented, submitted to NERC for review, and reported to FERC.

The self-logging program allows select registered entities with demonstrated effective internal control practices to log minimal risk noncompliance that would otherwise be individually self-reported. The registered entity must submit the log to its Regional Entity on a periodic basis for review of whether the registered entity has adequately identified and described the noncompliance, accurately assessed the risk, and appropriately mitigated the noncompliance. Once the review process is complete, the minimal risk issue is resolved as a compliance exception absent additional risk factors or other issues.

The experience of the ERO to date has shown that logs increase visibility into noncompliance detected and corrected by the registered entity, as registered entities are more likely to record instances of noncompliance on their logs than self-report them to the ERO. Further, the program fosters efficiency and reduces certain formal administrative processes associated with individual Self-Reports, allowing entities to focus more resources on protecting Bulk-Power System reliability than on administrative compliance processes.

The self-logging program is consistent with the "identify, assess, and correct" tenet that noncompliance that is self-identified through internal controls, corrected through a strong

compliance culture, and documented by the registered entity should not be resolved through the enforcement process or incur a penalty, absent a higher risk to the Bulk-Power Systems. The risk-based enforcement processes are superior to the "identify, assess, and correct" language because they inform the Regional Entities, NERC, and FERC about the deficiencies registered entities may experience in complying with NERC's Reliability Standards. This information offers more timely feedback to Regional Entities on the effectiveness of the programs the registered entities have established for compliance with NERC's Reliability Standards.

NERC and the standard drafting team thus determined that the most appropriate response to the directive in Order No. 791 was to remove the "identify, assess, and correct" language from the CIP Reliability Standards and apply the risk-based CMEP to all of the CIP Reliability Standards. Attachment H hereto provides further information regarding the application of the risk-based CMEP to the CIP Reliability Standards.

B. Security Controls for Low Impact BES Cyber Systems

i. Order No. 791

The CIP Version 5 Standards require responsible entities to identify and categorize BES Cyber Systems using a new methodology based on whether a BES Cyber System has a low, medium, or high impact on the reliable operation of the Bulk Electric System.[36] As the Commission recognized, categorizing BES Cyber Systems in this manner, with all BES Cyber Systems categorized as at least low impact, offers more comprehensive protection of the Bulk Electric System.[37] The adoption of the low impact category will expand the protections offered

[36] *See* Reliability Standard CIP-002-5.1.

[37] Order No. 791 at P 107.

by the CIP Version 5 Standards to additional devices that, if compromised, could adversely affect the reliable operation of the Bulk Electric System.

Under the CIP Version 5 Standards, once a responsible entity identifies and categorizes a BES Cyber System under Reliability Standard CIP-002-5.1, the entity must comply with the requirements included in Reliability Standards CIP-003 to CIP-011 corresponding to the BES Cyber System's impact category. As the Commission noted, however, the only requirement in the CIP Version 5 Standards applicable to low impact BES Cyber Systems is Reliability Standard CIP-003-5, Requirement R2, which provides:

> R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months:
>
> 2.1 Cyber security awareness;
>
> 2.2 Physical security controls;
>
> 2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
>
> 2.4 Incident response to a Cyber Security Incident.

In Order No. 791, the Commission expressed concern that the CIP Version 5 Standards do not require specific controls for assets containing low impact BES Cyber Systems nor do they contain objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities under Reliability Standard CIP-003-5, Requirement R2.[38] The Commission stated that the lack of specific controls or objective criteria "introduces an unacceptable level of ambiguity and potential inconsistency into the compliance process, and creates an unnecessary gap in reliability." The Commission stated that "[t]his ambiguity will make it difficult for registered

[38] Order No. 791 at P 107.

entities to develop, and NERC and the regions to objectively evaluate, the effectiveness of procedures developed to implement Reliability Standard CIP-003-5, Requirement R2."[39] The Commission thus directed NERC to develop modifications to CIP Version 5 Standards to address this concern.

The Commission stated that NERC could address this concern in a number of ways, including:

1. requiring specific controls for low impact assets, including subdividing the assets into different categories with different defined controls applicable to each subcategory;

2. developing objective criteria against which the controls adopted by responsible entities can be compared and measured in order to evaluate their adequacy, including subdividing the assets into different categories with different defined control objectives applicable to each subcategory;

3. defining with greater specificity the processes that responsible entities must have for low impact facilities under Reliability Standard CIP-003-5, Requirement R2; or

4. another equally efficient and effective solution.[40]

ii. Proposed Modifications

To address the Commission's concern regarding the protections for low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6 includes additional specificity regarding the controls that responsible entities must implement for protecting their low impact BES Cyber Systems. As described below, proposed Reliability Standard CIP-003-6, Requirement R2 requires entities to implement controls necessary to meet specific security objectives with respect to four subject matter areas: (1) cybersecurity awareness, (2) physical security controls, (3) electronic access controls, and (4) Cyber Security Incident response. These four subject matter areas are those that were previously included in Reliability Standard CIP-003-5, Requirement R2 and that

[39] Order No. 791 at P 108.

[40] *Id*. at P 108.

the standard drafting team identified as necessary to address the risks associated with low impact BES Cyber Systems. Proposed Reliability Standard CIP-003-6, Requirement R1 also requires responsible entities to develop cybersecurity policies applicable to their low impact BES Cyber Systems to communicate management's expectations for cybersecurity across the organization.

The underlying principle of the CIP Version 5 Standards and the categorization of BES Cyber Assets as high, medium, or low impact is to require responsible entities to protect their BES Cyber Systems commensurate with the risks they present to the reliable operation of the Bulk Electric System (i.e., commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the Bulk Electric System). The goal is to focus industry resources on those areas that provide the most reliability benefit. As the Commission recognized in determining that an inventory of low impact BES Cyber Systems should not be required, given their lower risk profile, the requirements applicable to low impact BES Cyber Systems should not be overly burdensome to divert resources away from the protection of medium and high impact BES Cyber Systems.[41]

Consistent with that framework, the standard drafting team sought to develop requirements for low impact BES Cyber Systems that help mitigate the risks associated with those systems while also ensuring that responsible entities could continue to devote the necessary resources to protect their high and medium impact BES Cyber Systems. Accordingly, in contrast to the requirements applicable to high and medium impact BES Cyber Systems, the requirements applicable to low impact BES Cyber Systems may be implemented at the asset level (i.e., the protections would be applied to the site or location, such as Control Centers, Transmission stations or substations, and Generation plants, identified according to Reliability Standard CIP-002-5.1 that contain one or

[41] Order No. 791 at P 111.

more low impact BES Cyber Systems, not necessarily each BES Cyber Asset at those sites). If the low impact requirements were required to be applied at the device level, responsible entities would essentially be required to develop an inventory of low impact BES Cyber Systems, undercutting the goal of focusing industry resources on those areas that provide the greatest benefits to reliability.

Further, the standard drafting team concluded that focusing on the four subject matter areas listed above will have the greatest cybersecurity benefit for low impact BES Cyber Systems without diverting resources necessary for the protection of high and medium impact BES Cyber Systems. As discussed below, requiring entities to: (1) regularly reinforce cybersecurity awareness and best practices across the organization; (2) establish protections to control physical access; (3) establish electronic access controls to limit inbound and outbound communication; and (4) implement Cyber Security Incident response plans will help mitigate the risk and impact of cyber-attacks targeting low impact BES Cyber Systems.

Considering the large number and diversity of low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6, Requirement R2 provides responsible entities the flexibility to implement security controls for low impact BES Cyber Systems in the manner that best suits the needs and characteristics of their organization, so long as the responsible entity can demonstrate that it designed its controls to meet the ultimate security objectives. The standard drafting team concluded that attempts to overly prescribe specific controls for low impact BES Cyber Systems would be problematic given the diversity of low impact BES Cyber Systems and likely inhibit the development of innovative security controls. By articulating clear security objectives, however, the ERO and the Commission will have a basis from which to judge the sufficiency of the controls ultimately adopted by a responsible entity.

Reliability Standard CIP-003-6, Requirement R2 provides that "[e]ach Responsible Entity with at least one asset identified in CIP-002-5.1 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that includes the sections in Attachment 1" to the proposed Reliability Standard. Attachment 1 provides as follows:

> Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.
>
> Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.
>
> Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).
>
> Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.
>
> Section 3. Electronic Access Controls: Each Responsible Entity shall:
>
> 3.1 For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and
>
> 3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.
>
> Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:
>
> 4.1 Identification, classification, and response to Cyber Security Incidents;
>
> 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and

subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

The protections required by Requirement R2, Attachment 1 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The following is a discussion of each section in Attachment 1:

Section 1 requires responsible entities to develop and implement a plan to reinforce good cybersecurity practices within their organization. The standard drafting team found that regular communication emphasizing cybersecurity practices can significantly improve an entity's cybersecurity posture. To that end, Section 1 requires responsible entities to take measures to reinforce cybersecurity practices at least once every 15 months. The responsible entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics, so long as the responsible entity can demonstrate that its reinforcement activities are designed to raise cybersecurity awareness and promote a culture of security. The topics can include the physical security of BES Cyber Systems as well as technology-specific topics.

Section 2 addresses the physical security of low impact BES Cyber Systems, requiring responsible entities to document and implement methods to control physical access to: (1) low impact BES Cyber Systems; and (2) Low Impact BES Cyber System Electronic Access Points (or LEAPs), if any. A LEAP, which is a proposed term for inclusion in the NERC Glossary, is essentially an interface that controls electronic access to an asset containing a low impact BES Cyber System or the low impact BES Cyber System. A LEAP is defined as:

> A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

The term Low Impact External Routable Connectivity (or LERC), which is also a proposed term for inclusion in the NERC Glossary, is defined as

> Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).[42]

The responsible entity has the discretion to select the method used to control physical access based on organizational need. As discussed in the Guidelines and Technical Basis section of proposed Reliability Standard CIP-003-6, the responsible entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use facility-level perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or set up controls in the specific areas where low impact BES

[42] The exclusion of point-to-point communications between intelligent electronic devices was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Cyber Systems are located, such as control rooms or control houses. The controls to be implemented are necessarily dependent on the type of facility in question (e.g., limiting physical access to BES Cyber Systems at a wind generating facility spread across many acres of land requires a different set of controls than those required at a Transmission station). Regardless of the method chosen or the types of assets to be protected, the physical access controls must be designed to meet the overall security objective of limiting physical access to those individuals that need to be in a particular location to carry out the functions of the organization, whether it be a system operator or a vendor that needs to service a particular device.

Section 3 requires responsible entities to establish electronic boundary protections for low impact BES Cyber Systems that have bi-directional routable protocol communication with, or Dial-up Connectivity to, devices external to the asset containing the low impact BES Cyber Systems. The boundary protections are intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. Considering the wide array of low impact BES Cyber Systems and the risk-based approach to protecting different types of BES Cyber Systems, the standard drafting team focused the electronic access controls on access external to the asset containing the low impact BES Cyber System and not on inter-asset communication. From a risk perspective, controlling the accessibility to or from the asset containing the low impact BES Cyber System significantly reduces the scale of threats to low impact BES Cyber Systems.

Pursuant to Section 3, if there is LERC, then a responsible entity must implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access. The

Guidelines and Technical Basis section of the proposed Reliability Standard describes situations where LERC exists:

> …LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to, logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session, even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication from or to the low impact BES Cyber System.

The Guidelines and Technical Basis section also provides examples of electronic access controls that would meet the security objectives, such as implementing a LEAP with explicitly defined inbound and outbound access permissions or using a host-based firewall to control the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in an external network.[43] Fundamentally, the goal is to ensure that low impact BES Cyber Systems are adequately separated from general purpose business networks and not accessible from the internet.

Responsible entities have flexibility in the method they use to control electronic access. As described in the Guidelines and Technical Basis section, in selecting an interface to control LERC (i.e., the LEAP), entities could use, for example, (1) the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, (2) the internal interface on a router that has implemented an access control list, or (3) another security device. Responsible entities also have flexibility with respect to the location of the LEAP, which is not required to reside at the

[43] The Guidelines and Technical Basis section also provides examples of situations that would lack sufficient access controls to meet the security objective.

asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP for every asset containing low impact BES Cyber Systems. Rather, responsible entities can have a single Cyber Asset containing multiple LEAPs that control LERC for multiple assets containing low impact BES Cyber Systems. Regardless of the method chosen to implement the LEAP, responsible entities must meet the ultimate security objective of permitting only necessary inbound and outbound bi-directional routable protocol access.

Section 4 requires responsible entities to have one or more documented response plans that set forth the actions they must take when responding to a Cyber Security Incident associated with low impact BES Cyber Systems. These response plans will help ensure that entities can respond efficiently and effectively to any Cyber Security Incidents at assets containing low impact BES Cyber Systems and, in turn, limit any adverse impact. Additionally, by requiring entities to determine whether a Cyber Security Incident is a Reportable Cyber Security Incident (requiring notification to the ES-ISAC), the Cyber Security Incident response plans will help ensure that other responsible entities are aware of the incident and take appropriate action to protect their BES Cyber Systems. The Cyber Security Incident response plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can use a single enterprise-wide plan for all low impact BES Cyber Systems.

For each of these sections, those responsible entities that have multi-impact-rated BES Cyber Systems can use the policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plans. This approach may create efficiencies for entities and allow them to better manage their resources. Moreover, in recognition of the diverse set of low impact BES Cyber Systems, responsible entities

can develop the cybersecurity plan(s) required by CIP-003-6, Requirement R2 either by individual asset or groups of assets.

In addition to the plans required by Requirement R2, proposed Reliability Standard CIP-003-6, Requirement R1, Part 1.2 retains the requirement that responsible entities develop management-approved cybersecurity policies for their assets containing low impact BES Cyber Systems. These policies must cover the same four subject matter areas (cybersecurity awareness, physical security controls, electronic access controls, and Cyber Security Incident response) and must be reviewed and approved by the CIP Senior Manager at least once every 15 calendar months. Proposed Reliability Standard CIP-003-6, Requirement R1 does not dictate the form or content of these policies. The responsible entity has the flexibility to develop a single comprehensive cybersecurity policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail related to the required topics in lower level documents in its documentation hierarchy. Under either scenario, however, the purpose of these policies is to communicate the responsible entity's management goals, objectives, and expectations for the protection of low impact BES Cyber Systems and establish a culture of security and compliance across the organization. These policies, together with the plans required under Requirement R2, provide a framework for implementing operational, procedural, and technical safeguards for securing low impact BES Cyber Systems commensurate with the risks they present.

C. Protection of Transient Devices

i. Order No. 791

In Order No. 791, the Commission directed NERC to modify the CIP Version 5 Standards to develop requirements that protect transient devices (e.g., thumb drives and laptop computers)

that fall outside the definition of BES Cyber Asset.[44] The FERC-approved definition of BES Cyber Asset provides, in relevant part:

> A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

The purpose of the 30-day exemption is to exclude transient devices from the full suite of cyber security protections applicable to BES Cyber Assets in the CIP Version 5 Standards. As the Commission agreed in Order No. 791, given that transient devices are portable and frequently connected and disconnected from systems, it would be unduly burdensome to protect transient devices in the same manner as BES Cyber Assets.[45]

Nevertheless, the Commission expressed concern as to whether the CIP Version 5 Standards provide adequately robust protection from the risks posed by transient devices, such as the introduction of malicious code. While the Commission acknowledged that the CIP Version 5 Standards already require that entities protect their BES Cyber Systems from malicious code, no matter the source, the Commission stated that "relying on a single security control to protect information systems is contrary to the fundamental cyber security concept of defense-in-depth." The Commission thus directed NERC to modify the CIP Version 5 Standards to addresses the risks posed by transient devices.

The Commission stated that the requirements should recognize that transient devices, unlike BES Cyber Assets, are generally portable and frequently connected and disconnected from systems. The Commission also "expects NERC to consider the following security elements when designing a Reliability Standard for transient devices: (1) device authorization as it relates to users

---

[44] Order No. 791 at PP 132-36.

[45] *Id*. at P 133.

and locations; (2) software authorization; (3) security patch management; (4) malware prevention; (5) detection controls for unauthorized physical access to a transient device; and (6) processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact)."

ii. Proposed Modifications

Consistent with Order No. 791 and to improve the defense-in-depth protections of the CIP Reliability Standards, the proposed Reliability Standards include specific requirements to mitigate the risks associated with transient devices. As most BES Cyber Systems are already isolated from external public or untrusted networks pursuant to the CIP Version 5 Standards, the use of transient devices is a potential vehicle for cyber-attacks. As the Commission recognized, "transient devices have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations" and, because these devices can move between ESPs, they could spread malware across a responsible entity's various BES Cyber Systems absent appropriate controls.[46] Using transient devices, however, is often the only way for responsible entities to transport files to and from secure areas to maintain, monitor, or troubleshoot BES Cyber Systems.

Accordingly, as described further below, NERC revised its CIP Reliability Standards, consistent with Order No. 791, to require entities to: (1) develop plans and implement cybersecurity controls to protect Transient Cyber Assets and Removable Media associated with their high impact and medium impact BES Cyber Systems and associated PCAs (CIP-010-2, Requirement R4); and (2) train their personnel on the risks associated with using Transient Cyber Assets and Removable Media (CIP-004-6, Requirement R2, Part 2.1). The purpose of the proposed revisions is to: (1) prevent unauthorized access to and the use of transient devices; (2)

[46] Order No. 791 at P 135.

mitigate the risk of vulnerabilities associated with unpatched software on such devices; and (3) mitigate the risk of the introduction of malicious code on such devices.

The standard drafting team determined that applying the proposed requirements to transient devices associated with high and medium impact BES Cyber Systems will help ensure that responsible entities appropriately focus their resources on protecting those BES Cyber Systems that, if compromised, present the greatest risks to reliability and warrant the defense-in-depth protections discussed in Order No. 791. The standard drafting team concluded that the application of the proposed transient devices requirements to transient devices associated with low impact BES Cyber Systems was unnecessary, and likely counterproductive, given the risks low impact BES Cyber Systems present to the Bulk Electric System. As discussed above, the standard drafting team sought to develop requirements for low impact BES Cyber Systems that mitigate the risks associated with those systems while ensuring that industry could still devote the necessary resources to protecting medium and high impact BES Cyber Systems. Applying the proposed transient devices requirements to low impact BES Cyber Systems could divert resources away from protecting medium and high BES Cyber Systems.

To manage risks associated with the use of Transient Cyber Assets and Removable Media across impact levels, however, the standard drafting team explicitly required responsible entities to implement the security controls before connecting such devices to high and medium impact BES Cyber Systems and their associated PCAs. As such, if a responsible entity uses the same Transient Cyber Assets and Removable Media across all impact levels, the risks posed by these devices are mitigated at all impact levels.

The following is a discussion of the proposed definitions associated with the proposed requirements applicable to transient devices and a description of those requirements.

a. Proposed Definitions Related to Transient Devices

To define and clarify the types of transient devices subject to the CIP Reliability Standards, NERC is proposing to add the following two terms to the NERC Glossary: (1) Transient Cyber Asset, and (2) Removable Media. The proposed definition of Transient Cyber Asset is:

> A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Examples of Transient Cyber Assets include, but are not limited to, diagnostic test equipment, packet sniffers, equipment used for BES Cyber System maintenance, equipment used for BES Cyber System configuration, or equipment used to perform vulnerability assessments. Transient Cyber Assets can be one of many types of devices, including a specially-designed device for maintaining equipment in support of the Bulk Electric System or a platform, such as a laptop, desktop, or tablet computer, which interfaces with or runs applications that support BES Cyber Systems.

The proposed definition of Removable Media is:

> Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

The standard drafting team also revised the definitions for BES Cyber Asset and PCA to remove the 30-day exemption. The proposed definition of Transient Cyber Asset obviates the need for the 30-day exemption as it covers those Cyber Assets that would otherwise have been subject to the 30-day exemption and specifically states that a Transient Cyber Asset is not included

in a BES Cyber System and is not a PCA. As defined, Transient Cyber Assets and Removable Media do not provide reliability services and are not part of the BES Cyber System to which they are connected.

b. Proposed Requirements Applicable to Transient Cyber Assets and Removable Media

To protect BES Cyber Systems from the risks associated with transient devices, proposed Reliability Standard CIP-010-2, Requirement R4 requires entities to document and implement a plan for managing and protecting Transient Cyber Assets and Removable Media. Specifically, Requirement R4 provides that "[e]ach responsible entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, [to] implement, except under CIP Exceptional Circumstances, one or more documented plans for Transient Cyber Assets and Removable Media that include the sections in Attachment 1" to the proposed Reliability Standard. Attachment 1 sets forth the content that responsible entities must include in their plan(s). As described below, Attachment 1 does not prescribe a standard method or set of controls that each entity must implement to protect its transient devices. Instead, Attachment 1 requires responsible entities to meet certain security objectives by implementing the controls that the responsible entity determines necessary to meet its affirmative obligation to protect its transient devices. This approach provides the responsible entity the flexibility to implement the controls that best suit the needs and characteristics of its organization. To comply with Requirement R4, however, the responsible entity must be able to demonstrate that its selected controls were designed to meet the ultimate security objectives outlined in Attachment 1.

Under Attachment 1, responsible entities' plans must address the following three areas:

1. Protections for Transient Cyber Assets managed by the Responsible Entity.
2. Protections for Transient Cyber Assets managed by a party other than the Responsible Entity (e.g., vendors or contractors).

3. Protections for Removable Media.

These three sections reflect the standard drafting team's recognition that the security controls required for a particular transient device must account for the functionality of that device and/or whether the responsible entity or a third party manages the device. Because Transient Cyber Assets and Removable Media have different capabilities, they present different levels of risk to the Bulk Electric System, and the protections required under the proposed Reliability Standards must reflect those differences. For instance, Transient Cyber Assets are subject to vulnerabilities associated with unpatched software, while Removable Media are not. Similarly, the standard drafting team recognized that because a responsible entity lacks complete control over Transient Cyber Assets managed by a third party, it cannot implement the procedures for those devices (e.g., the responsible entity has limited authority to patch software on a device owned and managed by a third party).[47] The responsible entity, however, still has the responsibility to mitigate the risks associated with Transient Cyber Assets managed by a third party prior to connection. Accordingly, the standard drafting team established different requirements for Transient Cyber Assets managed by the responsible entity and those managed by a third-party, as well as for Removable Media.[48]

The following is a discussion of the security objectives and/or protections applicable to each of these sections:

Transient Cyber Assets Managed by the Responsible Entity: Attachment 1 provides as follows regarding Transient Cyber Assets managed by the responsible entity:

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

---

[47] Many responsible entities rely on third-party vendors or contractors to provide support services to BES Cyber Systems.

[48] Given the functionality of Removable Media, the standard drafting team concluded that it was not necessary to distinguish between Removable Media managed by the responsible entity and those managed by a third party. That is because, no matter who manages Removable Media, the same type of security controls can be applied (e.g., the scanning of a thumb drive prior to connection).

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 1.1 requires responsible entities to document how they plan to manage their Transient Cyber Assets. While responsible entities have the flexibility to manage their Transient

Cyber Assets on a continuous basis or on an as-needed basis, requiring entities to document how they are managing Transient Cyber Assets will help ensure that applicable personnel understand the steps they need to take prior to using a particular Transient Cyber Asset. Such documentation will thus help reduce the likelihood that a Transient Cyber Asset will be connected to a BES Cyber Asset, a network within an ESP, or a PCA absent the proper protections.

Section 1.2 requires entities to limit the use of their Transient Cyber Assets to a specific set of authorized users, locations, and business functions. For authorizing users, responsible entities may authorize by individual, department, or specific job function. Similarly, when authorizing locations, the entity may specify a discrete location or a group of locations. Lastly, when authorizing uses for an individual or group of Transient Cyber Assets, the entity may specify one or more business functions or tasks for which the device may be used. As part of this process, the entity should also specify any software or application packages authorized to be included on the device that are necessary to perform the specified business function or task (e.g., data transfer, vulnerability assessment, maintenance, or troubleshooting) as well as the authorized network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections).

By controlling who may use a Transient Cyber Asset, and where and for what purpose that Transient Cyber Asset may be used, entities will reduce the chances that Transient Cyber Assets could spread malware across their BES Cyber Systems. For example, if an entity restricts the use of certain laptop computers to Control Centers with high impact BES Cyber Systems and only includes software and applications on the laptop computer used for troubleshooting purposes, the entity not only limits the opportunity for that laptop computer to be the vehicle for a cyber-attack but also limits the potential impact if it were to be used as a vehicle in a cyber-attack.

Section 1.3 creates an affirmative obligation on each responsible entity to take the necessary steps to mitigate the risk of vulnerabilities posed by unpatched software on its Transient Cyber Assets. Entities must use one or more of the following methods to achieve this security objective: (1) security patching, including manual or managed updates;[49] (2) live operating system and software executable only from read-only media;[50] (3) system hardening;[51] or (4) other methods that are equally as effective at mitigating software vulnerabilities. While entities have significant flexibility to choose whatever method best suits their needs, regardless of the method(s) chosen, each responsible entity must be able to demonstrate that it used appropriate methods to meet its affirmative obligation to mitigate software vulnerabilities on its Transient Cyber Assets.

The phrase "per Transient Cyber Asset capability" is used in Section 1.3 and elsewhere in Attachment 1 to clarify that if a particular mitigation method cannot be implemented for a particular Transient Cyber Asset, an entity is not required to use that particular method. Nevertheless, the entity continues to be responsible for implementing an equally effective method, if necessary and capable, to meet the ultimate security objective.

Section 1.4 obligates entities to document and implement processes to mitigate the risk of introducing malicious code into a BES Cyber System through a Transient Cyber Asset. Entities must use one or more of the following methods to achieve this security objective: (1) antivirus

---

[49] The responsible entity has the flexibility to include its Transient Cyber Assets in its enterprise-wise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset.

[50] This method will help mitigate software vulnerabilities by creating protected operating systems that cannot be modified to deliver malicious software.

[51] System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function.

software, including manual or managed updates of signatures or patterns;[52] (2) application whitelisting;[53] or (3) other equally effective methods. While entities have the flexibility to choose whatever method best suits their needs, each responsible entity must be able to demonstrate that it used appropriate methods to meet its affirmative obligation to mitigate the risks of introducing malicious code. When addressing malicious code protection, the responsible entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered on a Transient Cyber Asset, it must be removed or mitigated to prevent it from being introduced into a BES Cyber Asset or BES Cyber System.

Lastly, Section 1.5 requires entities to document and implement processes for mitigating the risk of unauthorized use of Transient Cyber Assets. If there is an unauthorized use of a Transient Cyber Asset, there is an increased risk that the device could be tampered with or exposed to malware. Entities must use one or more of the following methods to achieve the security objective of mitigating the risk of unauthorized use: (1) restrict physical access; (2) full-disk encryption with authentication; (3) multi-factor authentication; or (4) other equally effective methods.[54] Again, regardless of the method(s) chosen, each responsible entity must be able to demonstrate that it used appropriate methods to meet its affirmative obligation to mitigate the risks of unauthorized use.

---

[52] Entities have the flexibility to deploy antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns, or scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

[53] Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.

[54] Additional information on each of these methods is provided in the Guidelines and Technical Basis section of proposed Reliability Standard CIP-010-2.

Transient Cyber Assets Managed by a Third Party: Responsible entities often use third-party vendors and contractors to provide support services to BES Cyber Systems. The third-party vendors or contractors frequently use Transient Cyber Assets to provide such services. As such, the standard drafting team recognized that to mitigate the risks associated with the use of Transient Cyber Assets, it was also necessary to require entities to take steps to protect their BES Cyber Systems from the risks associated with using Transient Cyber Assets managed by a third party. Because responsible entities have less control over those devices, the standard drafting team recognized that the requirements applicable to such devices must account for that lack of control.[55] Accordingly, the requirements related to such devices are in a separate section and focus on reviewing the third party's controls and taking any necessary follow-up action if the entity deems such controls insufficient to mitigate the risks associated with such devices. Specifically, Attachment 1 provides the following for Transient Cyber Assets managed by a third party:

> **Section 2.** Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.
>
> **2.1** Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):
>
> - Review of installed security patch(es);
> - Review of security patching process used by the party;
> - Review of other vulnerability mitigation performed by the party; or
> - Other method(s) to mitigate software vulnerabilities.
>
> **2.2** Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):
>
> - Review of antivirus update level;
> - Review of antivirus update process used by the party;

[55] For instance, the responsible entity cannot limit the users of the device, the locations at which the device is used, or the purposes for which the device is used.

- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Sections 2.1 and 2.2 have the same security objective as Sections 1.3 and 1.4, respectively, requiring responsible entities take the necessary steps to mitigate software vulnerabilities on Transient Cyber Assets and the introduction of malicious code. Because Sections 2.1 and 2.2 address devices managed by a third party, however, the focus is on reviewing the security controls used by the third party to ensure there are sufficient protections in place. Following the entity's review under Sections 2.1 and 2.2, Section 2.3 requires the entity to determine whether any additional actions are necessary to mitigate the risks associated with using a third party's Transient Cyber Asset. If additional actions are necessary, the entity must take such actions prior to connecting the Transient Cyber Asset to an applicable system. Regardless of the method(s) and/or actions the entity chooses to implement under Section 2, the entity must be able to demonstrate that it used appropriate methods to meet the overall security objective.

Removable Media: Although, as noted above, Removable Media do not have the same functionality as Transient Cyber Assets, the standard drafting team recognized that such devices can be the source of a cyber-attack and must be protected. For instance, while Removable Media are not subject to software vulnerabilities, it is possible for such devices to spread malware. As the Commission pointed out in Order No. 791, there were "two recent situations where malware was introduced into electric generation industrial control systems (ICS) through removable media

(i.e. a USB drive) that was being used to back-up a control system environment and updates."[56] Accordingly, under Section 3 of Attachment 1, entities are required to document and implement processes for: (1) limiting who may use Removable Media and at what locations; and (2) mitigating the threat of introducing malicious code to high or medium impact BES Cyber Systems and their associated PCAs. Specifically, Section 3 of Attachment 1 provides as follows:

> **Section 3.** Removable Media
>
> **3.1** Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:
>
> **3.1.1.** Users, either individually or by group or role; and
>
> **3.1.2.** Locations, either individually or by group.
>
> **3.2.** Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:
>
> **3.2.1.** Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and
>
> **3.2.2.** Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

Section 3.1 requires entities to limit the use of Removable Media to a specific set of authorized users and locations. When authorizing users, responsible entities may authorize by individual, department, or specific job function. Similarly, when authorizing locations, the entity may specify a discrete location or a group of locations.[57] By controlling who may use Removable Media and where Removable Media may be used, entities will reduce the chances that Removable Media could spread malware across their BES Cyber Systems.

---

[56] Order No. 791 at n.166.

[57] Given the limited functionality of Removable Media, as compared to Transient Cyber Assets, the standard drafting team concluded that it was unnecessary to require responsible entities to limit the uses of Removable Media as well.

Similar to Sections 1.4 and 2.2, discussed above, Section 3.2 requires entities to take the necessary steps to mitigate the risk of introducing malicious code into a BES Cyber System through Removable Media. Sections 3.2.1 and 3.2.2 create an affirmative obligation to (1) use methods to detect malicious code on Removable Media, and (2) mitigate the threat of any detected malicious code on Removable Media before connecting the device to a high impact or medium impact BES Cyber System or associated PCA. In implementing methods to detect malicious code, entities must use a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. Regardless of the methods chosen to detect and mitigate malicious code, the responsible entity must demonstrate that it used appropriate methods to meet the overall security objective of mitigating the risks of introducing malicious code through Removable Media.

In addition to the protections required by Reliability Standard CIP-010-2, Requirement R4, proposed Reliability Standard CIP-004-6, Requirement R2, Part 2.1 requires entities to provide training on the risks associated with Transient Cyber Assets and Removable Media. Specifically, Part 2.1 provides that entities must provide training on "[c]yber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and Removable Media." This training will help reinforce the protections required by proposed Reliability Standard CIP-010-2, Requirement R4.

D. Protection of Communication Networks

i. Order No. 791

In Order No. 791, the Commission approved the revised definition for the term "Cyber Asset," which removed reference to "communication networks."[58] The Commission concluded

[58] Order No. 791 at P 148. The currently-effective NERC Glossary definition of Cyber Asset is "[p]rogrammable electronic devices and communication networks including hardware, software, and data." The

that: (1) "it is not necessary to maintain the phrase 'communications network' within the text of the Cyber Asset definition to ensure that the programmable electronic components of these networks receive protection under the CIP Reliability Standards;" and (2) "maintaining the phrase "communication networks" within the Cyber Asset definition would likely cause confusion and possibly complicate the implementation of the CIP version 5 Standards, as many communication network components, such as cabling, cannot strictly comply with the CIP Reliability Standards."[59]

The Commission expressed concern, however, that the CIP Version 5 Standards do not explicitly address security controls needed to protect the nonprogrammable components of communication networks.[60] The Commission directed NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the protection of the nonprogrammable component of communication networks within one year of the date of Order No. 791.[61] The Commission stated that (1) the definition of communication networks should define what equipment and components should be protected, and (2) the new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks.

ii. Proposed Modifications

As the Commission has recognized, if entities do not take steps to secure nonprogrammable components of communication networks used to connect BES Cyber Assets, those components

definition of Cyber Asset approved in Order No. 791 is "[p]rogrammable electronic devices, including the hardware, software, and data in those devices."

59 Order No. 791 at P 148.

60 *Id*. at P 149. The Commission noted that other information security standards address the protection of communication mediums, for instance in NIST SP 800-53 Rev. 3, security control PE-4 includes examples of protecting communication medium including: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

61 *Id*. at P 150.

could be used to access BES Cyber Assets and ultimately compromise the reliable operation of the Bulk-Power System.[62] To address this concern, the proposed Reliability Standards require entities to implement security controls for nonprogrammable components of communication networks (e.g., cabling, wiring, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers) at Control Centers with high or medium impact BES Cyber Systems. The standard drafting team focused on nonprogrammable communication components at Control Centers with high or medium impact BES Cyber Systems because those locations present a heightened risk to the Bulk-Power System warranting the increased protections. As discussed above, the CIP Reliability Standards are designed to focus industry resources on protecting those BES Cyber Systems and associated devices or communication mediums that present increased risks to the reliable operation of the Bulk Electric System.

Proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10 provides that, for high impact BES Cyber Systems and their associated PCAs, and medium impact BES Cyber Systems at Control Centers and their associated PCAs, responsible entities must either physically secure nonprogrammable communication components that are located outside a PSP (e.g., by conduit, secured cable trays, or secured communication closets) or implement other effective protections (e.g., data encryption or circuit monitoring) to mitigate the risks associated with exposed nonprogrammable communication components. Specifically, Part 1.10 provides that responsible entities must take the following action:

> Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.

[62] Order No. 791 at PP 148-149; *North American Electric Reliability Corporation*, 142 FERC ¶ 61,203 (2013).

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:

- encryption of data that transits such cabling and components;
- monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
- an equally effective logical protection.

The protections required by Part 1.10 will reduce the possibility of tampering and the likelihood that "man-in-the-middle" attacks could compromise the integrity of BES Cyber Systems or PCAs at Control Centers with high or medium impact BES Cyber Systems. For example, responsible entities will now be required to protect cabling between a data center and a control room where the Cyber Assets in the data center and control room are in the same ESP but the cabling is outside a PSP. Proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10 applies only to nonprogrammable components outside of a PSP because nonprogrammable components located within a PSP are already subject to physical security protections by virtue of being within a PSP. Reliability Standard CIP-006-6, Requirements R1, R2, and R3 require entities to implement various security controls to restrict and manage physical access to PSPs.

Similarly, Part 1.10 only applies to nonprogrammable components used for connection between applicable Cyber Assets within the same ESP because Reliability Standard CIP-005-5 already requires logical protections for communications between discrete ESPs. For instance, under CIP-005-5, Requirement R2 responsible entities must do the following for Interactive Remote Access into an ESP: (1) use an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset; (2) use encryption

that terminates at an Intermediate System; and (3) require multi-factor authentication for all Interactive Remote Access sessions.

Responsible entities have the discretion as to the type of physical or logical protections to implement pursuant to CIP-006-6, Requirement R1, Part 1.10, provided that the protections are designed to meet the overall security objective. The standard drafting team provided this flexibility to allow entities to implement the physical security measure(s) that best suits their needs and to account for configurations where logical measures are necessary because the entity cannot implement physical access restrictions effectively. As the Commission has recognized, where physical security protections for communication mediums cannot be implemented effectively, logical measures may be an appropriate alternative to accomplishing the security objective.[63]

If the entity chooses to implement physical security measures, the entity must design such measures to effectively restrict physical access to the nonprogrammable communication components, such as the use of a padlock on a communications closet, armored cabling, or stainless steel or aluminum tube protecting the fiber inside an optical ground wire cable.[64] Regardless of the specific control(s) implemented, the entity must physically protect the entirety of the nonprogrammable communication component, including any termination points that may be outside of a defined PSP. Similarly, if an entity chooses to implement logical protections, the entity must design such measures to effectively mitigate the risks associated with exposed communication components.

---

63 *North American Electric Reliability Corporation*, 132 FERC ¶ 61,051 (2010).

64 As discussed in the Guidelines and Technical Basis section of the proposed Reliability Standard, these physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling or other nonprogrammable components.

Additionally, proposed Reliability Standard CIP-007-6, Requirement R1, Part 1.2 extends the requirement for entities to protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media to PCAs and nonprogrammable communications components associated with all high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers.[65] Pursuant to the proposed modification, the network ports included in the scope of Part 1.2 are not limited to those on the BES Cyber System itself but also include ports that exist on PCAs and nonprogrammable communication components, such as unmanaged switches, hubs, or patch panels, located within a PSP and an ESP. The extended applicability of Part 1.2 will strengthen the defense-in-depth approach provided by the CIP Reliability Standards by further minimizing the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.[66]

The proposed modification to Part 1.2 applies to nonprogrammable communication components within a PSP and an ESP for applicable BES Cyber Systems to allow for a scenario where the responsible entity implements an extended ESP covering multiple locations (with corresponding logical protections identified in CIP-006-6, Requirement R1, Part 1.10). The standard drafting team limited the applicability in this manner to clarify that responsible entities are not responsible for protecting nonprogrammable communication components outside of the responsible entity's control (i.e., components of a telecommunication carrier's network).

Finally, the standard drafting team concluded that it was not necessary to develop a definition of the phrase "communication network" to address the Commission's concerns

---

[65] The extension of Part 1.2 to PCAs and nonprogrammable communication components is consistent with NIST SP 800-53 Rev. 3, security control PE-4.

[66] The standard drafting team also revised Part 1.2 to capitalize the term "Removable Media."

regarding the protection of nonprogrammable components of communication networks. As the Commission recognized in its order remanding a proposed interpretation of Reliability Standard CIP-006-4, the term "communication network" is generally understood to encompass both programmable components and nonprogrammable components (i.e., a communication network includes computers peripherals, terminals, and databases as well as communication mediums such as wires).[67] In turn, any proposed definition would need to be sufficiently broad to encompass all components in a communication network as they exist now and in the future.[68] Rather than trying to circumscribe the exact components of a communication network in a NERC Glossary definition, the standard drafting team simply identified the types of equipment or components that entities must protect and proposed appropriate and reasonable controls to secure those components based on the risks they present to the Bulk Electric System.

The standard drafting team did not identify the need to use a broadly-defined term in the CIP Reliability Standards to accomplish the security objective to protect nonprogrammable communication components. Whether or not there is a NERC Glossary definition for the term "communication network," NERC's cybersecurity standards, as proposed, meet the ultimate security objective of protecting communication networks (both programmable and nonprogrammable communication network components). First, the CIP Version 5 Standards already include protections for programmable components of a communication network as BES Cyber Assets or PCAs, depending on their function and location. In addition, the proposed Reliability Standards include protections for cables and other the nonprogrammable

---

67 *North American Electric Reliability Corporation*, 142 FERC ¶ 61,203 at PP 13-14 (2013).

68 For example, NIST Special Publication 800-53, Revision 4 refers to the CNSSI 4009 definition of Network, which is "[i]nformation system(s) implemented with a collection of interconnected components."

communication components, as discussed above, to augment the existing protections for programmable communication components.

E. Enforceability of the Proposed Reliability Standards

The proposed Reliability Standards include VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standards. The VRFs and VSLs for the proposed Reliability Standards comport with NERC and Commission guidelines related to their assignment. Exhibit E provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

The proposed Reliability Standards also include measures that support each requirement by clearly identifying what is required and how the ERO will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[69]

V. EFFECTIVE DATE

NERC respectfully requests that the Commission approve the proposed Reliability Standards to become effective as set forth in the proposed Implementation Plan, provided in Exhibit B hereto. The proposed Implementation Plan is designed to match the effective dates of the proposed Reliability Standards with the effective dates of the prior versions of those Reliability Standards under the implementation plan for the CIP Version 5 Standards (the "CIP V5 Implementation Plan"), provided that responsible entities have at least three months to implement the proposed Reliability Standards. The purpose of this approach is to provide responsible entities regulatory certainty by limiting the time, if any, that the CIP Version 5 Standards with the

[69] Order No. 672 at P 327.

"identify, assess, and correct" language would be effective.[70] Specifically, pursuant to the CIP V5 Implementation Plan, the effective date of each of the CIP Version 5 Standards is April 1, 2016, except that the effective date for Requirement R2 of CIP-003-5, which addresses protections for low impact BES Cyber Systems, is April 1, 2017. Consistent with those dates, the proposed Implementation Plan provides that: (1) each of the proposed Reliability Standards "shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after" the effective date of the Commission's order approving the proposed Reliability Standard; and (2) responsible entities will not have to comply with the proposed requirements applicable to low impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) until April 1, 2017.

Where the standard drafting team identified the need for additional time for implementation of a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), however, the proposed Implementation Plan provides additional time for compliance with that particular section. Specifically, the standard drafting team provided additional implementation time for those sections of the proposed Reliability Standards that create entirely new obligations (as opposed to simply removing or slightly modifying an existing obligation) that require responsible entities to develop new processes and procedures and devote substantial resources for implementation. Because those new obligations were not anticipated when the effective dates for the CIP Version 5 Standards were established, the standard drafting team concluded that additional time was necessary to ensure an effective and efficient implementation of both the existing obligations in the CIP Version 5 Standards and the revisions proposed herein.

[70] If the timing of the Commission's order approving the proposed Reliability Standards results in the CIP Version 5 Standards with the "identify, assess, and correct" language taking effect, NERC would not enforce the "identify, assess, and correct" provisions during the short time that those standards would be effective.

The compliance dates for those particular sections of the proposed Reliability Standards represent the dates that entities must begin to comply with those sections, even where the Reliability Standards go into effect at an earlier date.

The following is a description of the compliance dates for each of the sections in the proposed Reliability Standards where the standard drafting team identified the need for additional time for implementation:

- *Reliability Standard CIP-003-6, Requirement R1, Part 1.2* – Entities are not required to comply with Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of CIP-003-6. This additional time is consistent with the implementation period provided in the CIP V5 Implementation Plan for obligations related to low impact BES Cyber Systems.

- *Reliability Standard CIP-003-6, Requirement R2* - Entities are not required to comply with Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of CIP-003-6. This additional time is consistent with the implementation period provided in the CIP V5 Implementation Plan for CIP-003-5, Requirement R2. Additionally, entities are not required to comply with Sections 2 and 3 of Attachment 1 to Reliability Standard CIP-003-6 until the later of September 1, 2018 or nine calendar months after the effective date of CIP-003-6. The standard drafting team concluded that an additional 17 months was necessary to ensure an effective implementation of the controls required by Section 2 and 3 of Attachment 1.

- *Reliability Standard CIP-006-6, Requirement R1, Part 1.10* – For new high or medium impact BES Cyber Systems at Control Centers which were not identified as Critical Cyber Assets under the currently effective version of the CIP Reliability Standards, responsible entities are not required to comply with Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6. Because entities were already protecting nonprogrammable components of communication networks under the currently effective version of the CIP Reliability Standards, the additional time for compliance with Part 1.10 only applies to communication components associated with newly identified BES Cyber Systems.

- *Reliability Standard CIP-007-6, Requirement R1, Part 1.2* – Responsible entities are not required to comply with Part 1.2 for their applicable PCAs and nonprogrammable communication components until nine calendar months after the effective date of Reliability Standard CIP-007-6. The standard drafting team concluded that an additional nine months was an appropriate time frame for compliance with the new obligations.

- *Reliability Standard CIP-010-2, Requirement R4* – Responsible entities are not required to comply with Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2. The standard drafting team concluded that an additional

nine months was an appropriate time frame for compliance with the new obligations associated with transient devices as entities will have to develop and implement new plans and processes to ensure effective compliance.

As to the proposed new and modified definitions, the Implementation Plan provides that their effective dates correspond to the compliance dates for those sections of the proposed Reliability Standards in which they are used. Specifically, the new and modified definitions associated with the transient devices directive (i.e., BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset) shall become effective on the compliance date for Reliability Standard CIP-010-2, Requirement R4. Similarly, the new and modified definitions associated with the low impact directive (i.e., Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity) shall become effective on the compliance date for Reliability Standard CIP-003-6, Requirement R2.

Lastly, the Implementation Plan provides that the retirement of Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1 shall become effective on the effective date of the proposed Reliability Standards.

VI. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve:

- the proposed Reliability Standards and associated elements included in Exhibit A, effective as proposed herein;
- the proposed Implementation Plan included in Exhibit B;
- the proposed new and revised definitions to be incorporated into the NERC Glossary included in Exhibit A; and
- the retirement of Commission-approved Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1, effective as proposed herein.

Respectfully submitted,

/s/ Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charles.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 13, 2015

Exhibit A

Proposed Reliability Standards

Reliability Standard CIP-003-6 Clean and Redline

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

See Implementation Plan for CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *policy* refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of *policies* also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2,	within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2)	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to CIP-003-6,	The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to CIP-003-6,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)	Requirement R2, Attachment 1, Section 2. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R3)	within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/2015	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

CIP-003-6 - Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIP-003-6 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1 - Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2 - Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
    a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
    b. The Cyber Asset, if any, containing a LEAP.

Section 3 - Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4 - Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);

2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-6, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through

successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control

- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

Using the list of assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse

or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or “If you see something, say something” campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) low impact BES Cyber Systems at assets containing low impact BES Cyber System(s) and (2) LEAPs, if any. If the LEAP is located within the BES asset and inherits the same controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems, the low impact BES Cyber Systems themselves, or LEAPs, if any. The Responsible Entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or

control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems, including LEAPs. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protections for low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. The term “electronic access control” is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude “point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems,” such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases “direct user-initiated interactive access or a direct device-to-device connection

to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and

other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

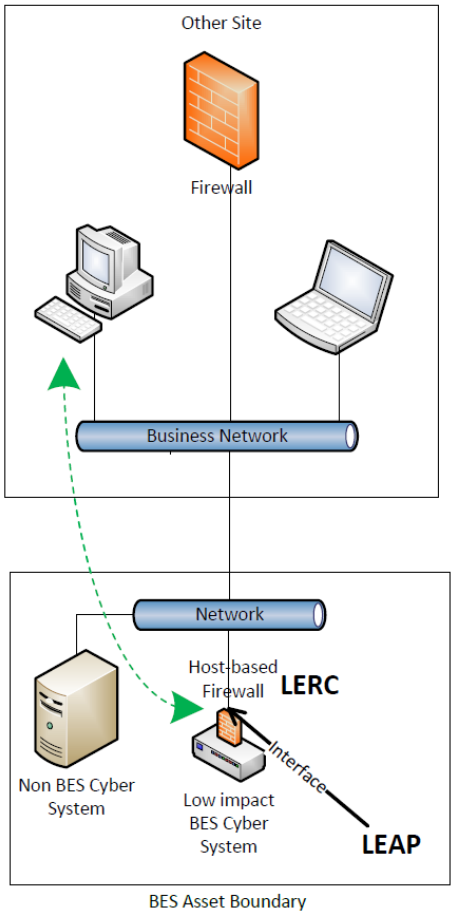
- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a “protocol break” so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.
- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

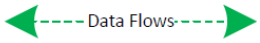
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System and the business network would not meet the intent of “controlling” inbound and

outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

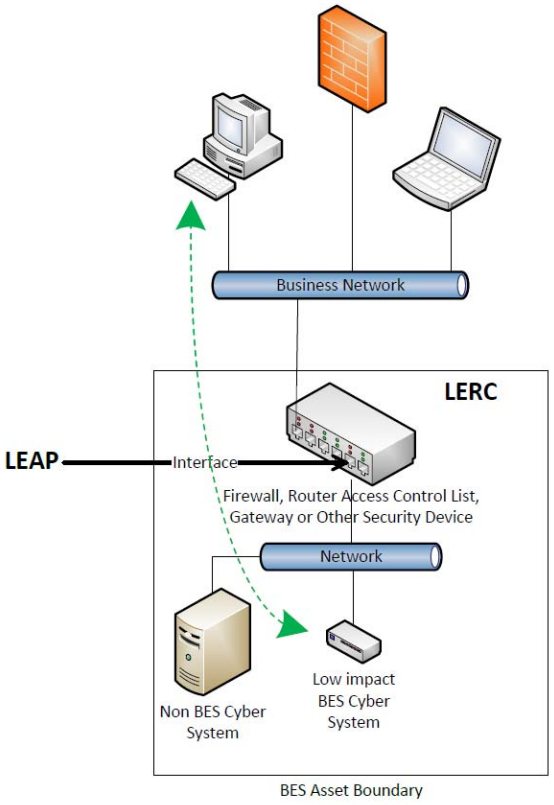
The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.





REFERENCE MODEL - 1

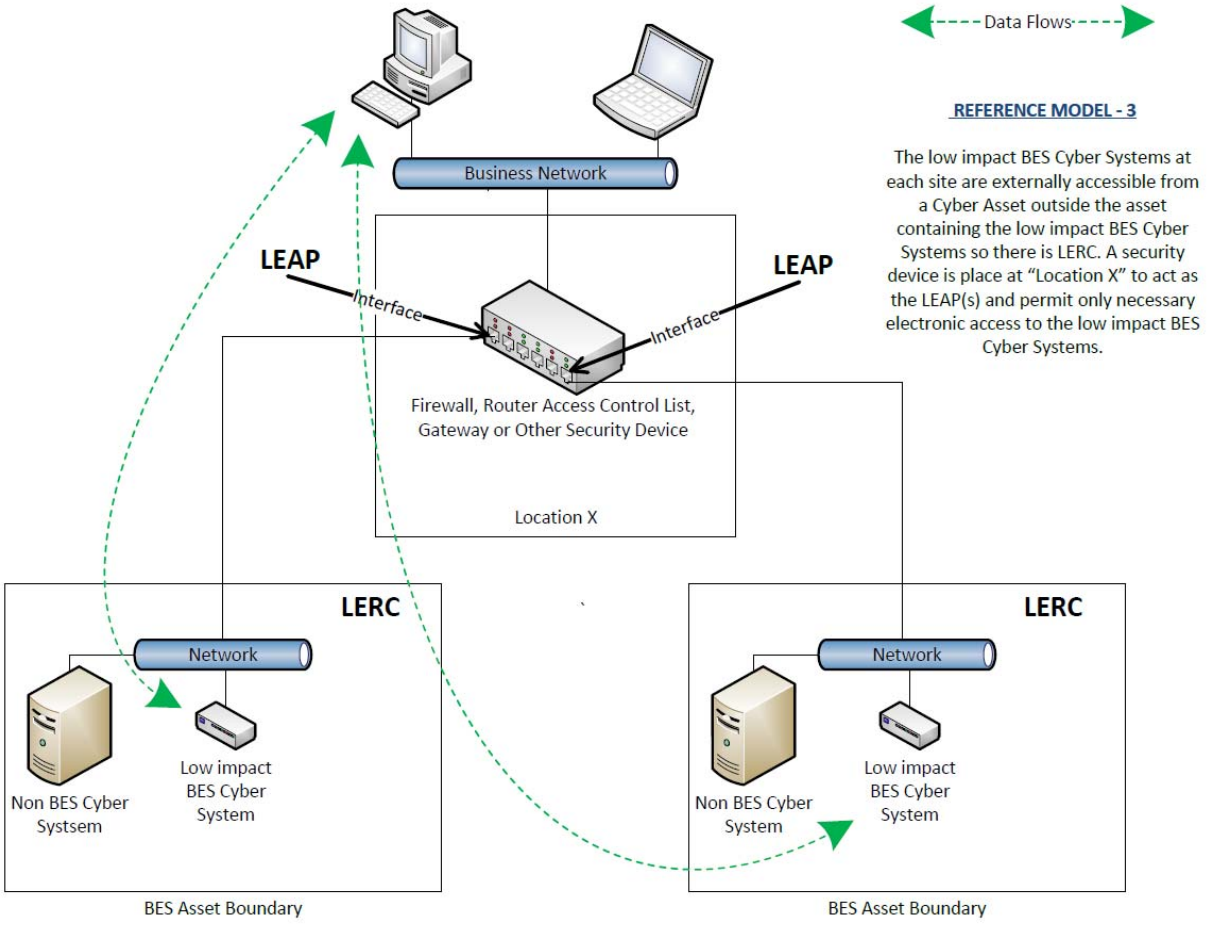
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

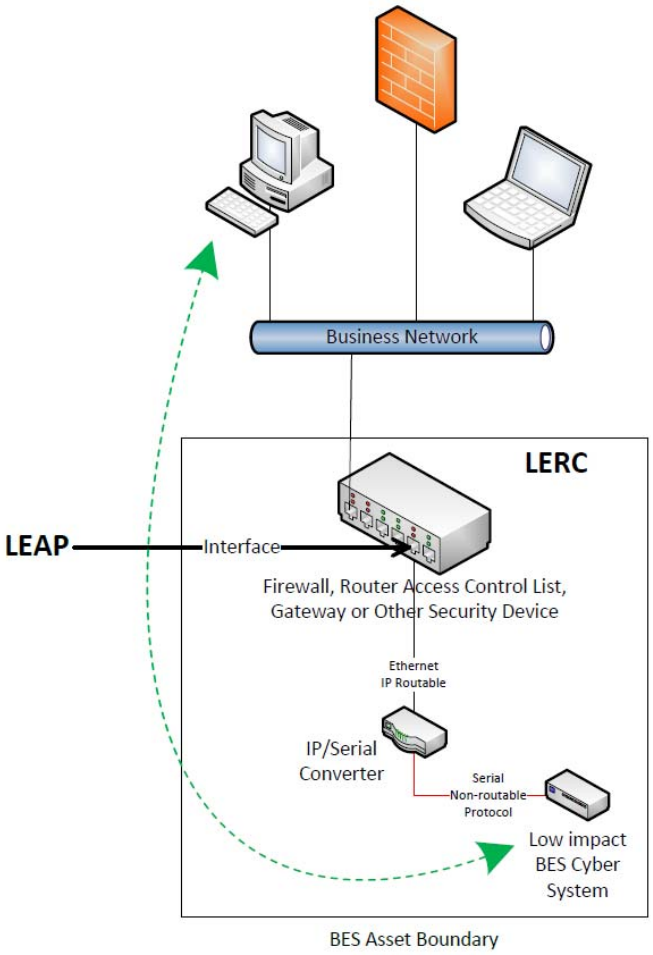


Data Flows

REFERENCE MODEL - 2

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

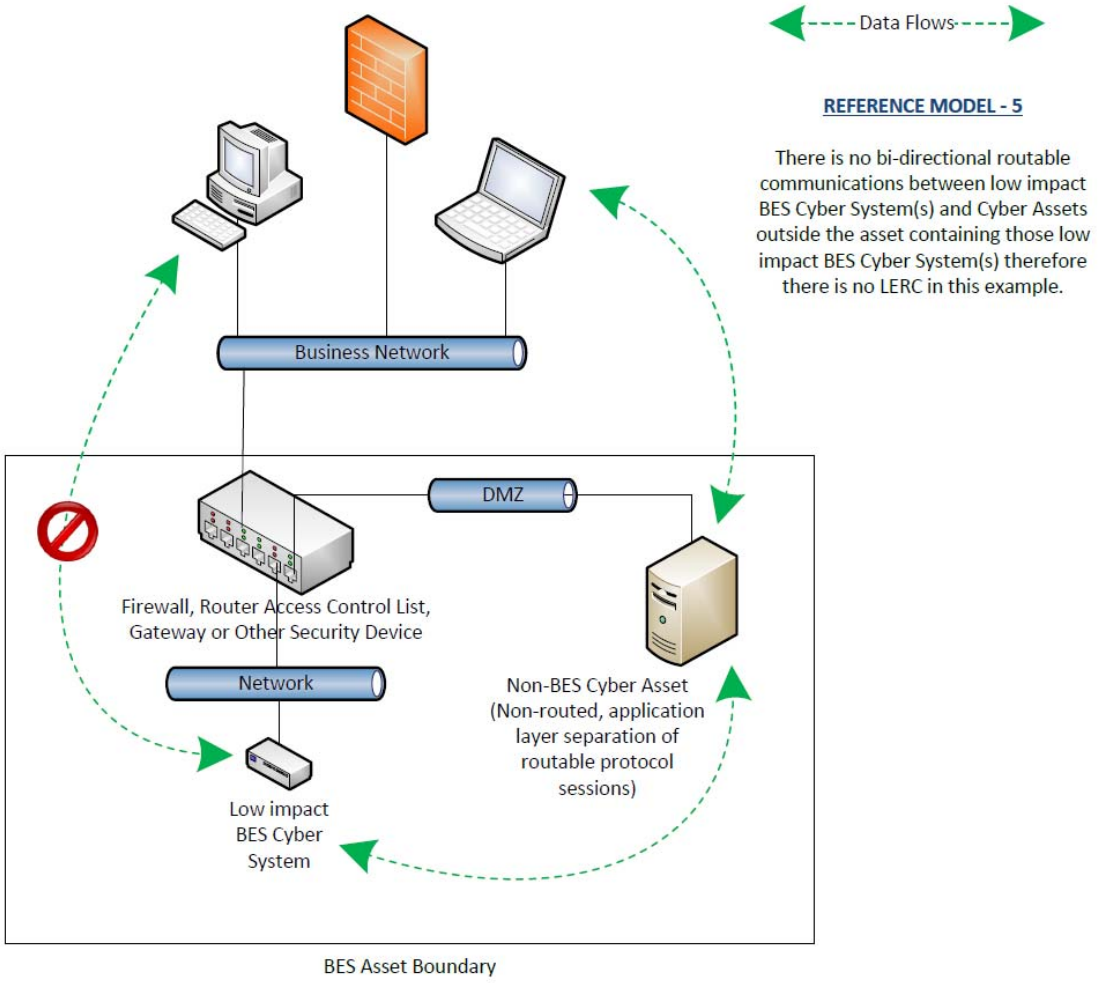

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

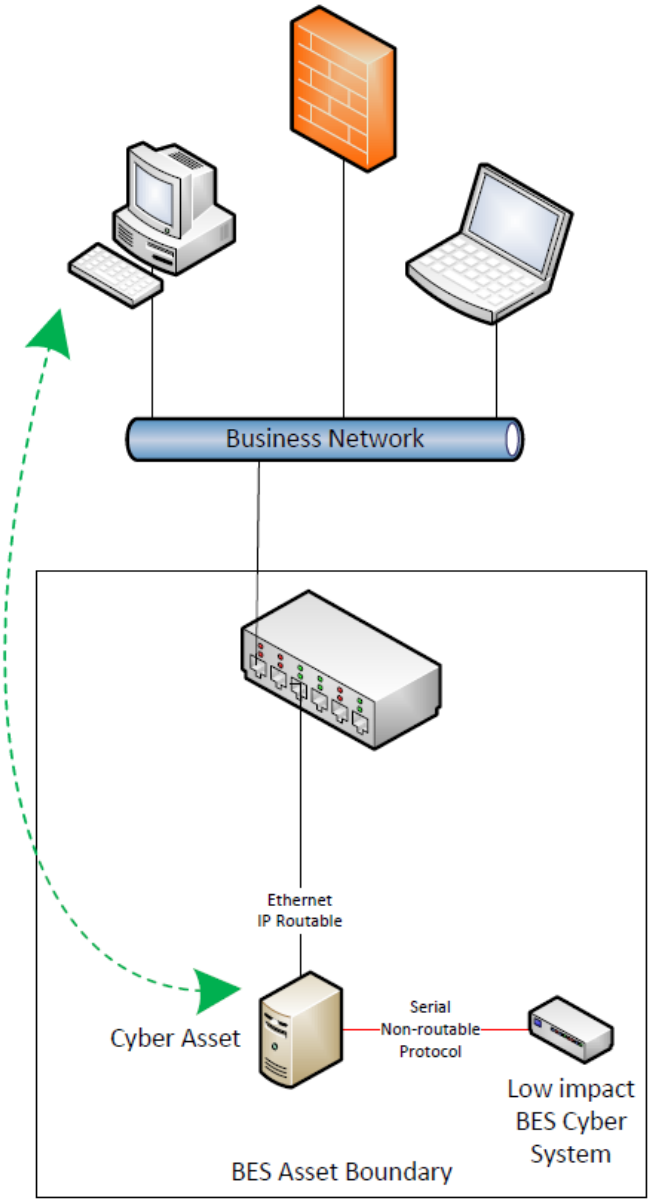


Data Flows

REFERENCE MODEL - 4

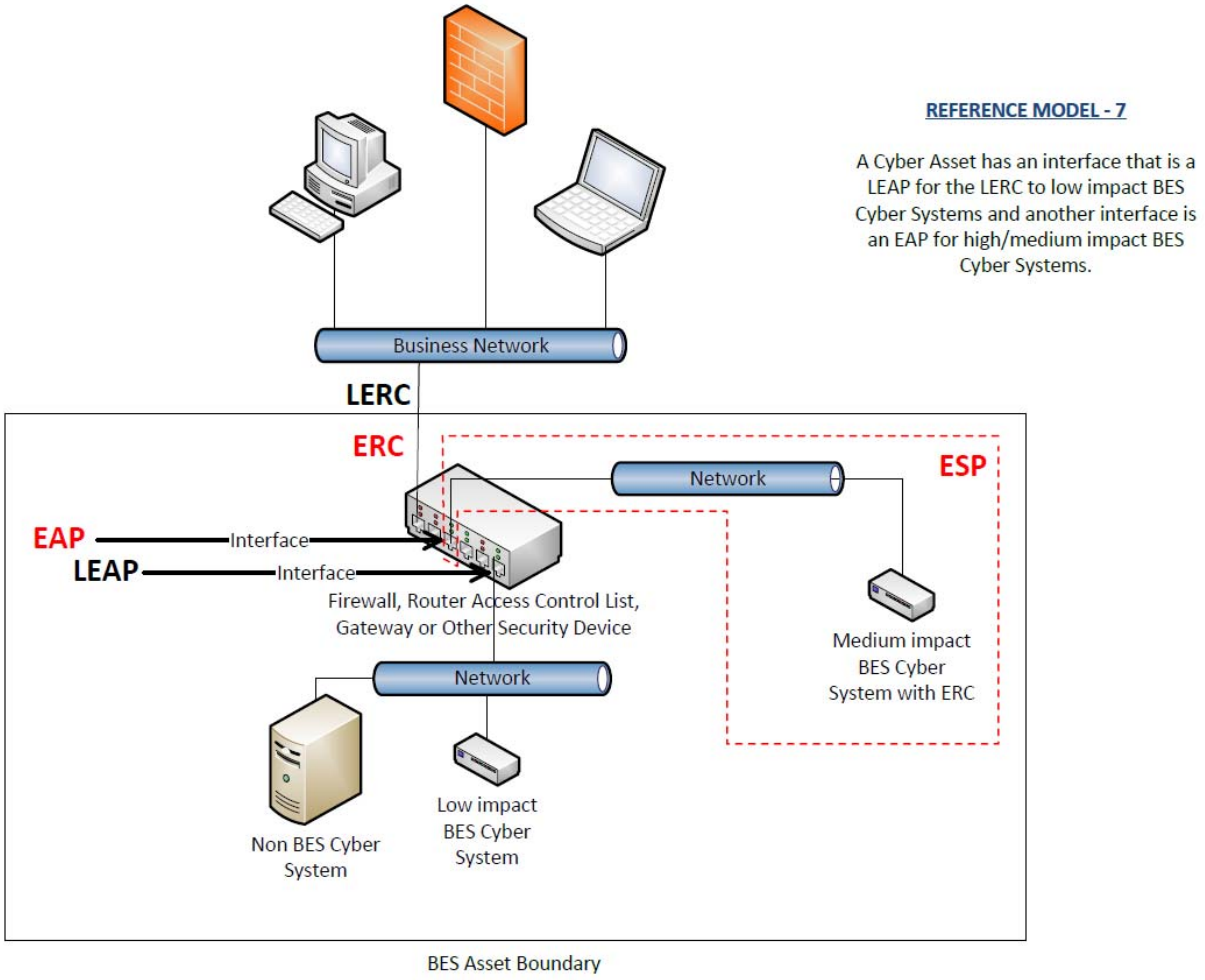
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.


Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber Systems, the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber Systems. The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber Systems. However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5~~5~~6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the ~~BES.~~Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-003-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESPs).

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. ~~5.~~ Effective Dates:

~~1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-003-6.

6. Background:

Standard CIP-003~~-5~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require ~~a minimum level of~~ organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred~~

The term *policy* refers to ~~as the *Version 5 CIP Cyber Security Standards*.~~ one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of *policies* also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high ~~and,~~ medium, and low impact BES Cyber Systems. For example, a single ~~training~~cyber security awareness program could meet the requirements ~~for training personnel~~ across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System.~~BES. A review of UFLS tolerances defined within ~~regional reliability standards~~Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity~~, for its high impact and medium impact BES Cyber Systems,~~ shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel ~~&~~and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity ~~for its assets~~with at least one asset identified in CIP-002~~-5, Requirement R1, Part R1.3,~~ containing low impact BES Cyber Systems shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented cyber security ~~policies that collectively address~~plan(s) for its low impact BES Cyber Systems that include the ~~following topics, and review and obtain CIP Senior~~

Manager approval for those policies at least once every 15 calendar months:sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Examples of evidence mayEvidence shall include, but are not limited to, one or more each of the documented cyber security policies and evidence of processes, procedures, or plansplan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy. plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve asAs defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ("" (CEA") unless) means NERC or the applicable entity is owned, operated, or controlled byRegional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEANERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance AuditAudits

Self-CertificationCertifications

Spot Checking

Compliance InvestigationInvestigations

Self-Reporting

ComplainComplaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate~~ within 18 calendar months of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	containing low impact BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber	previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented ~~and implemented one or more~~ its cyber security ~~policies~~plan(s) for its assets ~~with a~~containing low impact ~~rating that address only three of the topics as required by R2 and has identified deficiencies~~BES Cyber Systems, but ~~did not assess or correct the deficiencies.~~failed to document cyber security awareness according to CIP-003-	The Responsible Entity documented ~~and implemented one or more~~ its cyber security ~~policies~~plan(s) for its assets ~~with a~~containing low impact ~~rating that address only two of the topics as required by R2 and has identified deficiencies~~BES Cyber Systems, but ~~did not assess or correct the deficiencies.~~failed to reinforce cyber security practices at least once every 15	The Responsible Entity documented ~~and implemented~~ one or more Cyber Security Incident response plans within its cyber security ~~policies~~plan(s) for its assets ~~with a~~containing low impact ~~rating that address only one of the topics as required by R2 and has identified deficiencies~~BES Cyber Systems, but ~~did not assess or correct the deficiencies.~~failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-6,	The Responsible Entity ~~did not~~failed to document or implement ~~any~~one or more cyber security ~~policies~~plan(s) for its assets ~~with a~~containing low impact ~~rating that address the topics as required by R2. (R2)~~ ~~OR~~ ~~The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented ~~and implemented one or more~~ its cyber security ~~policies~~plan(s) for its assets ~~with a~~containing low impact ~~rating that address only three of the topics as required by R2~~BES Cyber Systems, but ~~did not identify, assess, or correct the deficiencies.~~failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2,	calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented ~~and implemented~~ one or more incident response plans within its cyber security ~~policies~~plan(s) for its assets ~~with a~~containing low impact ~~rating that address only two of the topics as required by~~BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents	Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit	~~impact rating as required by R2 within 18 calendar months of the previous review. (R2)~~ ~~OR~~ ~~The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the~~BES Cyber Systems according to CIP-~~Senior Manager within 18 calendar months of the previous approval.~~ 003-6, Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-56)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2) OR The Responsible Entity did not complete its review of the documented one or more documented Cyber Security Incident response plans within its cyber security policiesplan(s) for its assets with acontaining low impact rating as required by R2 within 15 calendar monthsBES Cyber Systems, but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	according to CIP-003-6, Requirement R2 but did not identify, assess, or correct the deficiencies., Attachment 1, Section 4. (R2) (R2) OR The Responsible Entity did not complete its review of the one or more documented its cyber security policiesplan(s) for its assets with acontaining low impact rating as required by R2 within 16 calendar monthsBES Cyber Systems, but did complete this review in less than or	inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for electronic access controls for its assets with acontaining low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with aBES Cyber	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~OR~~ ~~The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager~~failed to update each Cyber Security Incident response plan(s) within ~~15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)~~180 days according to CIP-003-6, Requirement R2,	~~equal~~failed to ~~17 calendar months of~~document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the ~~previous review. (R2)~~Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. OR The Responsible Entity ~~did not complete its approval of the one or more~~ documented its	Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact ~~rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review.~~BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity ~~did not complete its approval of the one or more~~ documented ~~cyber security policies~~the physical access controls for its assets ~~with a~~containing low impact	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2)	cyber security ~~policies~~plan(s) for its assets ~~with a~~containing low impact ~~rating as required by R2 by the CIP Senior Manager within 16 calendar months~~BES Cyber Systems, but ~~did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~failed to document physical security controls according to CIP-003-6, Requirement R2~~)~~, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	~~rating as required by R2 by the CIP Senior Manager within 17 calendar months~~BES Cyber Systems, but ~~did complete this approval in less than or equal~~failed to ~~18 calendar months of the previous approval.~~implement the physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4)~~ ~~OR~~ ~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4)~~	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~OR~~ The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/2015	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

CIP-003-6 - Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIP-003-6 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1 - Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2 - Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
    a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
    b. The Cyber Asset, if any, containing a LEAP.

Section 3 - Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections for any LEAP(s) are confined to only those the Responsible Entity deems necessary (e.g., by restricting IP addresses, ports, or services); and documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4 - Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);

2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

~~The~~In developing policies in compliance with Requirement R1, the number of policies and their ~~specific language are~~content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. ~~The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1.~~ The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering ~~these~~the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~5~~6, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-6, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the four subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-~~5~~6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-~~004~~003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements ~~from CIP-004 through CIP-011~~in NERC cyber security Reliability Standards, but ~~rather~~ to ~~put together~~develop a holistic cyber security policy appropriate ~~to~~for its organization. ~~The assessment through the Compliance Monitoring and Enforcement Program~~Elements of a policy ~~items~~ that extend beyond the scope of ~~CIP-004 through CIP-011 should~~NERC's cyber security Reliability Standards will not be considered candidates for potential violations~~. The Responsible Entity should consider the following for each~~ although they will help demonstrate the organization's internal culture of ~~the required topics in its~~compliance and posture towards cyber security~~ policy:~~.

For Part 1.1, the Responsible Entity should consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel ~~&~~and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

~~The Standard Drafting Team (SDT) has removed requirements~~Requirements relating to exceptions to a Responsible Entity's security policies ~~since~~were removed because it is a general management issue that is not within the scope of a reliability requirement. ~~The SDT considers it to be~~It is an internal policy requirement and not a reliability requirement. However, ~~the SDT encourages~~ Responsible Entities are encouraged to continue this practice as a component of ~~its~~their cyber security ~~policy~~policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~As with Requirement R1,~~Using the ~~number~~list of ~~policies~~ assets containing low impact BES Cyber Systems from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and ~~their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as~~ implement one or more cyber security plan(s) that addresses objective criteria for the protection of low impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a ~~general information security program for the entire organization or as components of specific~~program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level.

There are four subject matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs~~. The cyber security policy must cover in sufficient detail~~ used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. Guidance for each of the four ~~topical~~subject matter areas ~~required by CIP-003-5,~~ of Attachment 1 is provided below.

Requirement R2~~.~~, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The ~~Responsible Entity~~entity has ~~flexibility to develop a single comprehensive cyber security policy covering~~the discretion to determine the topics to be addressed and the manner in which it will communicate these topics~~, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy~~. As evidence of compliance, the Responsible Entity ~~would be expected to provide the high-~~should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) low impact BES Cyber Systems at assets containing low impact BES Cyber System(s) and (2) LEAPs, if any. If the LEAP is located within the BES asset and inherits the same controls outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems, the low impact BES Cyber Systems themselves, or LEAPs, if any. The Responsible Entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level ~~policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this~~ for access to the site or systems, including LEAPs. The requirement ~~can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (~~does not obligate an entity to specify a need for each access or authorization of a user for access.

Monitoring as a physical security control can be used as ~~of this writing) of reviewing~~a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a ~~statistical sample of systems is not necessary. The SDT also notes that in topic 2.3, the SDT uses the~~ controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of boundary protections for low impact BES Cyber Systems when the low impact BES Cyber Systems have bi-directional routable protocol communication or Dial-up Connectivity to devices external to the asset containing the low impact BES Cyber Systems. The establishment of boundary protections is intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System itself to reduce the risks associated with uncontrolled communication using routable

protocols or Dial-up Connectivity. The term "electronic access control" is used in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing. The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s).

The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude "point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems," such as IEC 61850 messaging. This does not exclude Control Center communication but rather excludes the communication between the intelligent electronic devices themselves. A Responsible Entity using this technology is not expected to implement a LEAP. This exception was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication to or from the low impact BES Cyber System.

When identifying a LEAP, Responsible Entities are provided flexibility in the selection of the interface on a Cyber Asset that controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, the internal interface on a router that has implemented an access control list (ACL), or other security device. The entity also has flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple

assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s).

In Reference Model 4, the communication flows through an IP/Serial converter. LERC is correctly identified in this Reference Model because the IP/Serial converter in this instance is doing nothing more than extending the communication between the low impact BES Cyber System and the Cyber Asset outside the asset containing the low impact BES Cyber System. In contrast, Reference Model 6 has placed a Cyber Asset that performs a complete break or interruption that does not allow the user or device data flow to directly communicate with the low impact BES Cyber System. The Cyber Asset in Reference Model 6 is preventing extending access to the low impact BES Cyber System from the Cyber Asset outside the asset containing the low impact BES Cyber System. The intent is that if the IP/Serial converter that is deployed only does a "pass-through" of the data flow communication, then that "pass-through" data flow communication is LERC and a LEAP is required. However, if that IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication can be sent to the low impact BES Cyber System, then that type of IP/Serial converter implementation is not LERC.

A Cyber Asset that contains interface(s) that only perform the function of a LEAP does not meet the definition of Electronic Access Control or Monitoring System (EACMS) associated with medium or high impact BES Cyber Systems and is not subject to the requirements applicable to an EACMS. However, a Cyber Asset may contain some interfaces that function as a LEAP and other interfaces that function as an EAP for high or medium impact BES Cyber Systems. In this case, the Cyber Asset would also be subject to the requirements applicable to the EACMS associated with the medium or high impact BES Cyber Systems.

Examples of sufficient access controls may include:

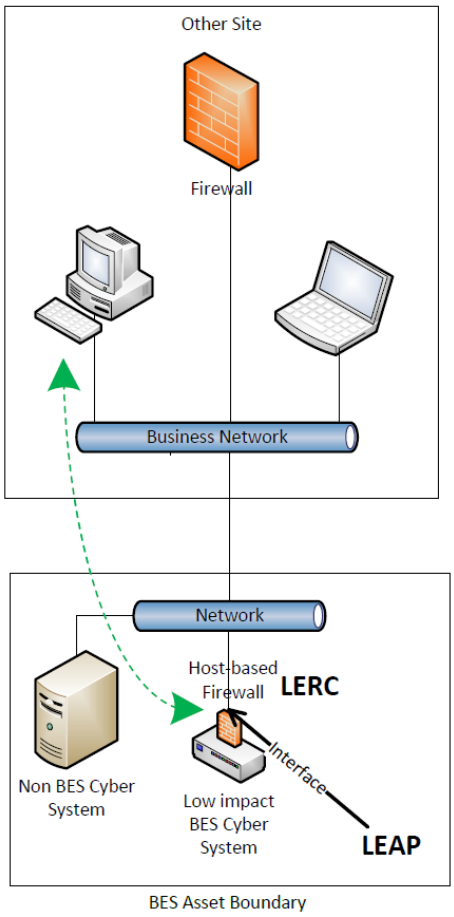
- Any LERC for the asset passes through a LEAP with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g., IP addresses, ports, or services).
- As shown in Reference Model 1 below, the low impact BES Cyber System has a host-based firewall that is controlling the inbound and outbound access. In this model, it is also possible that the host-based firewall could be on a non-BES Cyber Asset. The intent is that the host-based firewall controls the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in the business network.
- As shown in Reference Model 5 below, a non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that the non-BES Cyber Asset has provided a "protocol break" so that access to the low impact BES Cyber System is only from the non-BES Cyber Asset that is located within the asset containing the low impact BES Cyber System.

- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- An asset has LERC due to a BES Cyber System within it having a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- In Reference Model 5, using just dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System and the business network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security device on that non-BES Cyber Asset.

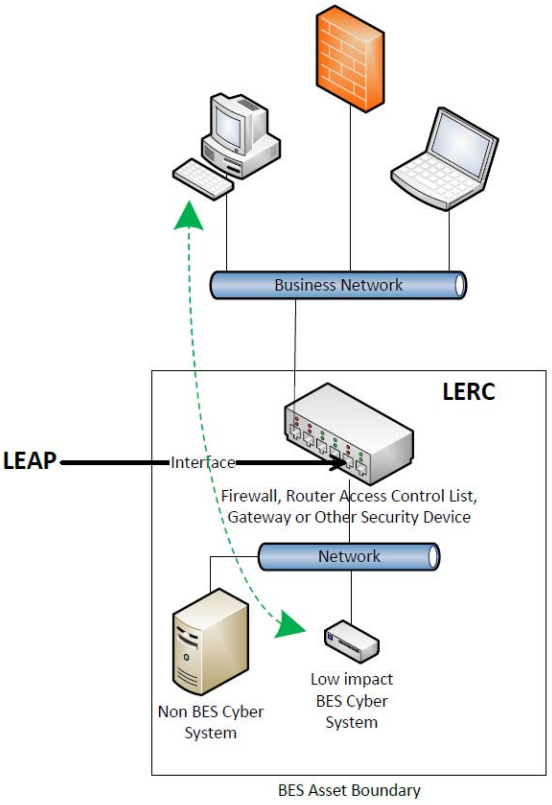
The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and for implementing a LEAP. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.



Data Flows

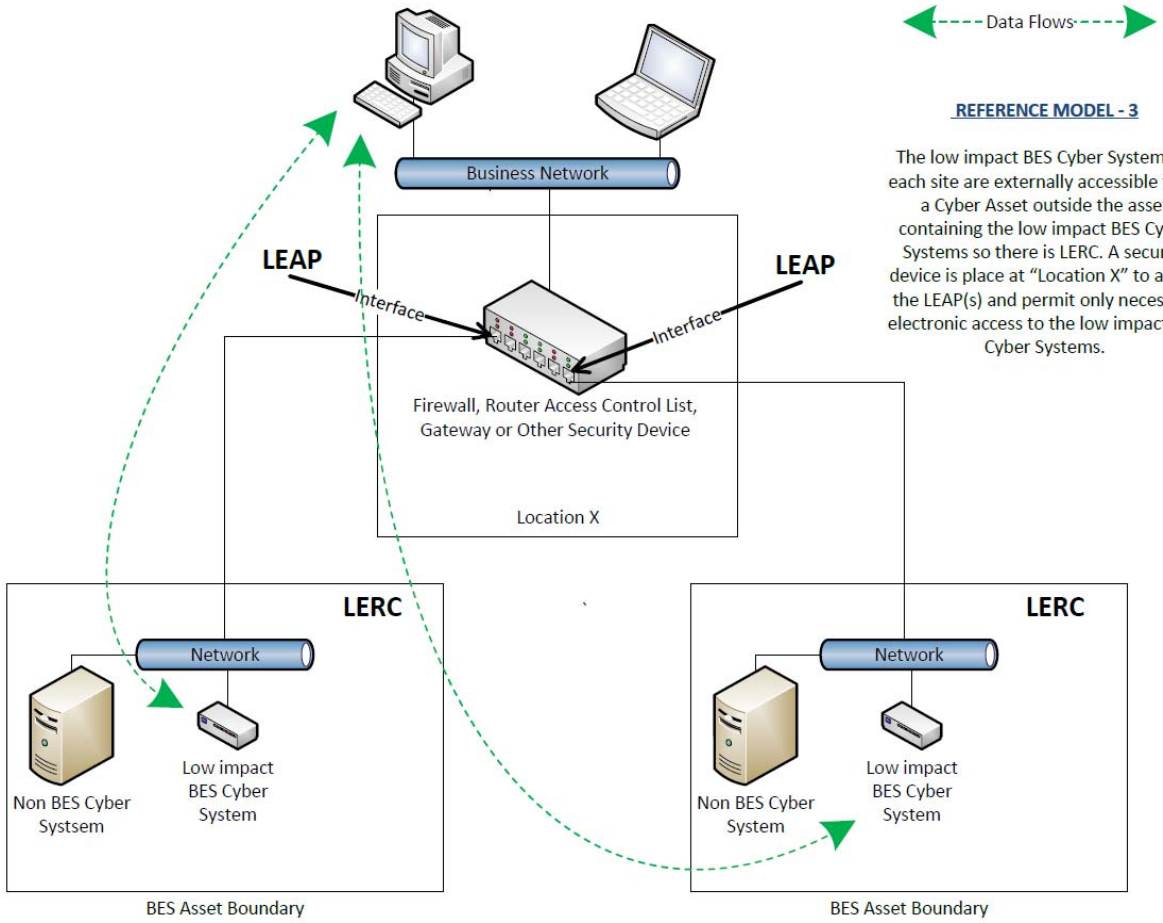
REFERENCE MODEL - 1

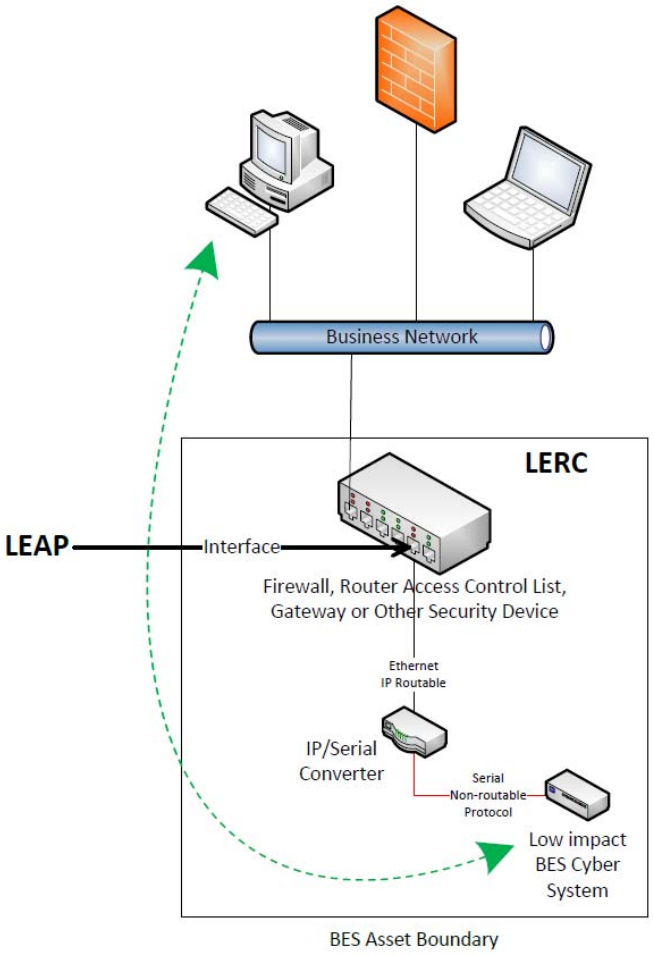
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.



REFERENCE MODEL - 2

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

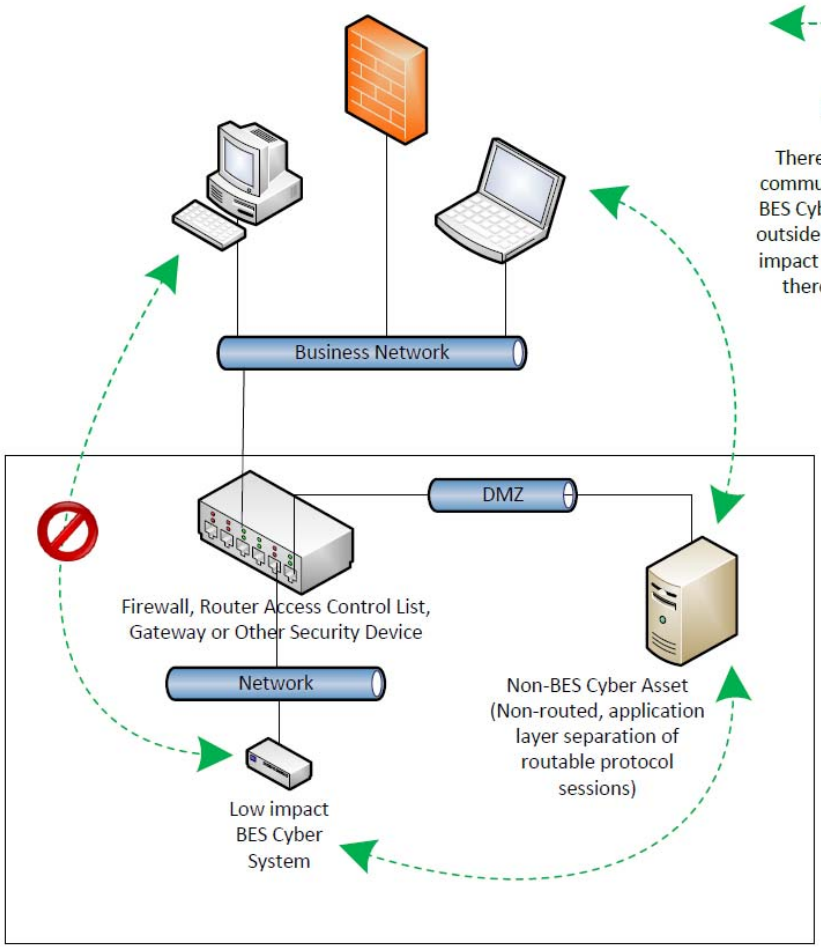

Data Flows
REFERENCE MODEL - 3
The low impact BES Cyber Systems at each site are externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber Systems so there is LERC. A security device is place at "Location X" to act as the LEAP(s) and permit only necessary electronic access to the low impact BES Cyber Systems.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router Access Control List, Gateway or Other Security Device
Location X
LERC
Network
Non BES Cyber Systsem
Low impact BES Cyber System
BES Asset Boundary
LERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary

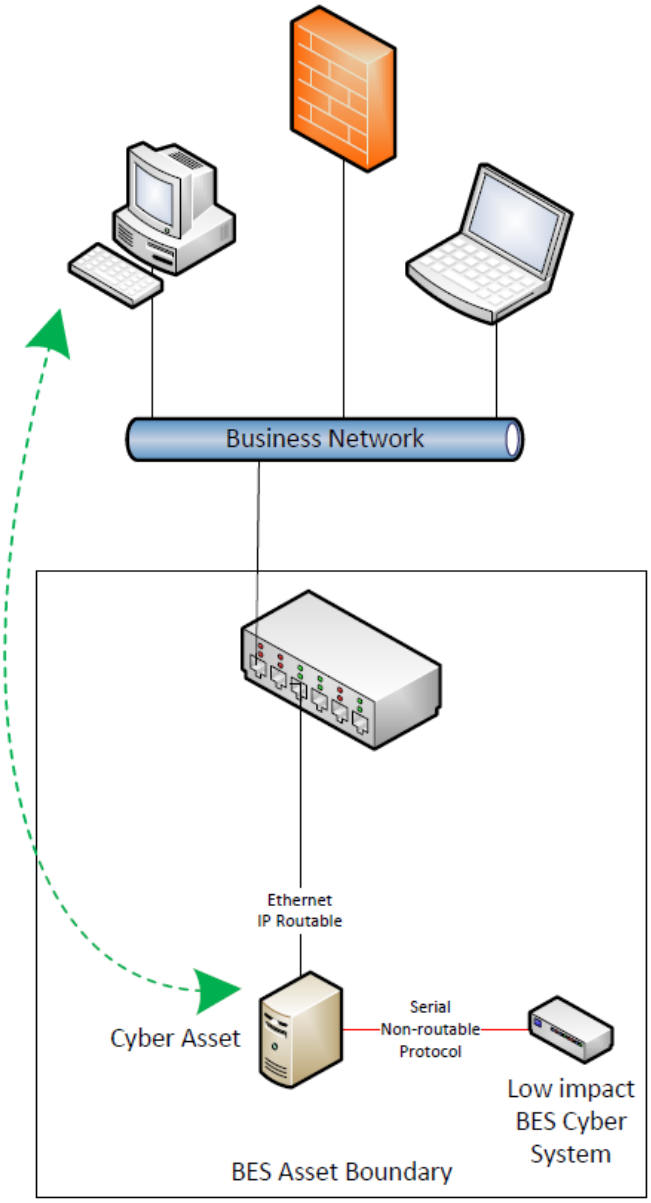


Data Flows

REFERENCE MODEL - 4

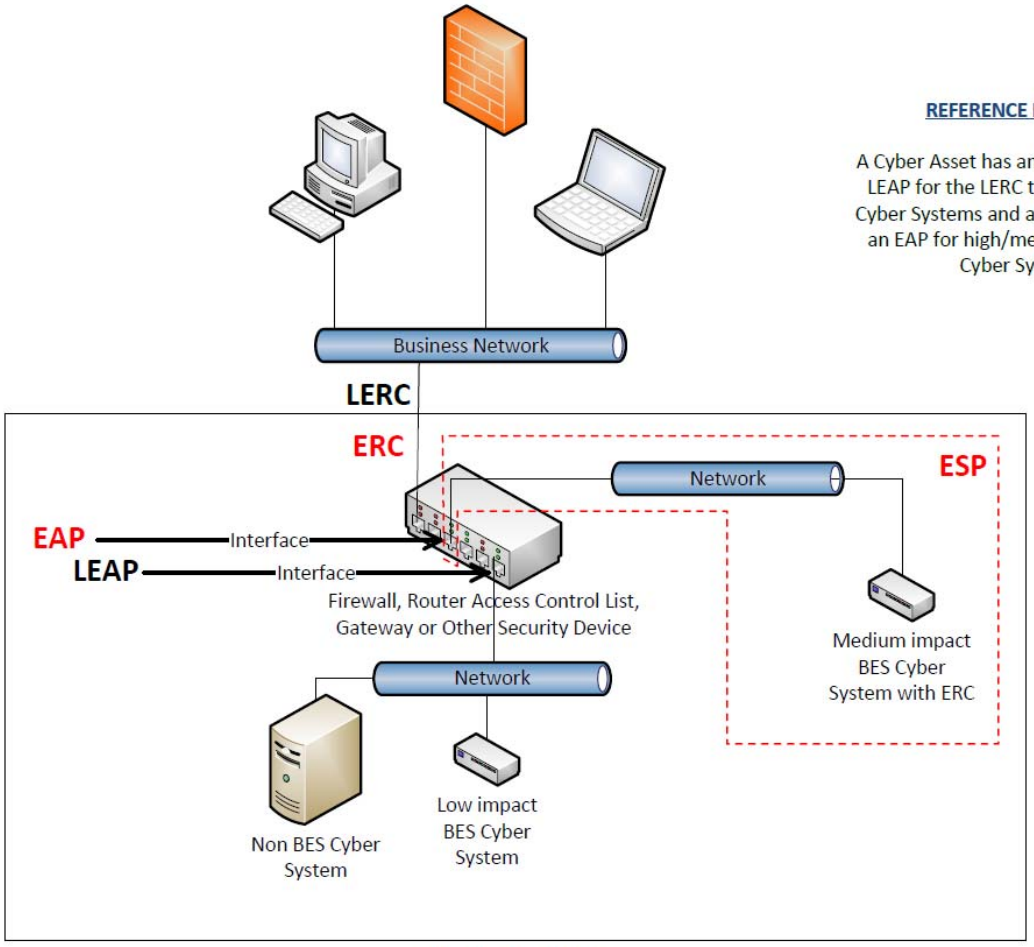
The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.


Data Flows
REFERENCE MODEL - 5
There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.
Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
Low impact BES Cyber System
BES Asset Boundary



REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.



Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber Systems, the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-~~5~~6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that ~~this~~the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~5~~6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity ~~should have~~ significant flexibility to adapt this requirement to ~~their~~its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records ~~provides~~shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the ~~standard's~~ requirements~~.~~ of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to ~~personnel who have authorized electronic access and/or authorized unescorted physical access to its~~a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the ~~standard's~~ requirements.

Annual review and approval of the cyber security ~~policy~~policies ensures that the ~~policy is~~policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

~~One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.~~

~~The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.~~

~~Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact

BES Cyber Systems. The cyber security plan(s) covers four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber Systems. However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the ~~senior manager~~CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

~~Version History~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~1/16/06~~	~~R3.2 — Change "Control Center" to "control center."~~	~~3/24/06~~
~~2~~	~~9/30/09~~	~~Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a responsible entity.~~ ~~Rewording of Effective Date.~~ ~~Changed compliance monitor to Compliance Enforcement Authority.~~	
~~3~~	~~12/16/09~~	~~Updated version number from -2 to -3~~ ~~Approved by the NERC Board of Trustees.~~	
~~3~~	~~3/31/10~~	~~Approved by FERC.~~	

~~4~~	~~1/24/11~~	~~Approved by the NERC Board of Trustees.~~	~~Update to conform to changes to CIP-002-4 (Project 2008-06)~~
~~5~~	~~11/26/12~~	~~Adopted by the NERC Board of Trustees.~~	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~
~~5~~	~~11/22/13~~	~~FERC Order issued approving CIP-003-5. (Order becomes effective 2/3/14.)~~	
~~5~~	~~4/2/14~~	~~Address directive in FERC Order 791 to modify VSLs for Requirements R1 and R2~~	~~R1 and R2 – VSLs~~

Reliability Standard CIP-004-6 Clean and Redline

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-6.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.4)	incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			locations, privileges were incorrect or unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR	access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the	access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR	termination action. (5.3)	date and time of the termination action. (5.3)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/2015	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

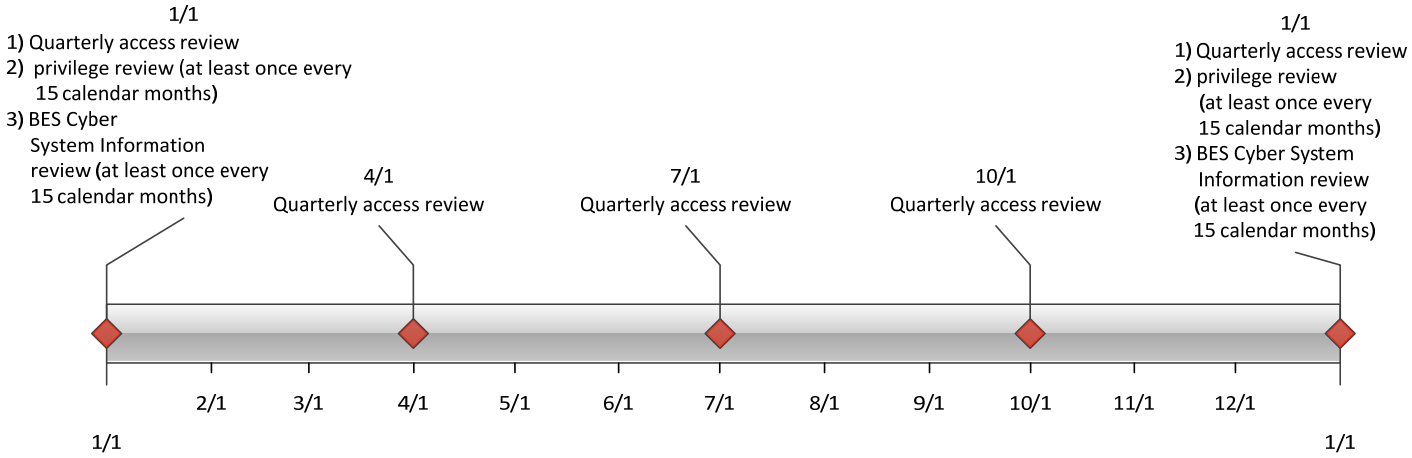
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such

authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-~~5.1~~6

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~5.1~~6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. ~~5.~~ Effective Dates:

~~1. **24 Months Minimum** – CIP-004-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-004-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-004-6.

6. Background:

Standard CIP-004~~-5.1~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards.*~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~.~~] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the ~~requirement's~~ common subject matter of the requirements.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement **, in a manner that identifies, assesses, and corrects deficiencies, . . .~~**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table~~. The documented processes themselves are~~

~~not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities~~.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System.~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies, a~~ one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment ~~programs~~program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~(""~~ (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Violation Investigations

Self-Reporting

~~• Complaint~~

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9~~; and did not identify, assess and correct the deficiencies.~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	~~and correct the deficiencies.~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies.~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized	~~and correct the deficiencies.~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies.~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies.~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access~~, and did not identify, assess and correct the deficiencies.~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies. (2.3)~~. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies. (2.3)~~. (2.3)	~~identify, assess and correct the deficiencies.~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies. (2.3)~~. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date~~, and did not identify, assess and correct the deficiencies. (2.3)~~. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals~~, and did not identify, assess, and correct the deficiencies.~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals~~, and did not identify, assess, and correct the deficiencies.~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual~~, and did not identify, assess, and correct the deficiencies.~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals~~, and did not identify, assess, and correct the deficiencies.~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals~~, and did not identify, assess, and~~	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals~~, and did not identify, assess, and correct the deficiencies.~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals~~, and did not identify, assess, and~~	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals~~, and did not identify, assess, and correct the deficiencies.~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals~~, and did not identify, assess, and correct the deficiencies.~~. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual~~, and did not identify, assess, and correct the deficiencies.~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	~~correct the deficiencies.~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals~~, and did not identify, assess, and correct the deficiencies.~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	~~correct the deficiencies.~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals~~, and did not identify, assess, and correct the deficiencies.~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals~~, and did not identify, assess, and correct the deficiencies.~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual~~, and did not identify, assess, and correct the deficiencies.~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies. (3.5)~~. (3.5)	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies. (3.5)~~. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals~~, and did not identify, assess, and correct the deficiencies.~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date ~~and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)~~. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual~~, and did not identify, assess, and correct the deficiencies.~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies. (3.5)~~. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies.~~. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies.~~. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter~~, and did not identify, assess and correct the deficiencies.~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies.~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies.~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	BES Cyber System Information is located~~, and did not identify, assess, and correct the deficiencies. (4.1)~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters~~, and did not identify, assess, and correct the deficiencies.~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies.~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies. (4.4)~~ . (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies. (4.4)~~ . (4.4)	role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies.~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies. (4.4)~~ . (4.4)			Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies. (4.4)~~ . (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies.~~. (5.3) OR The Responsible	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual~~, and did not identify, assess, and correct the deficiencies.~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals~~, and did not identify, assess, and correct the deficiencies.~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted	physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals~~, and did not identify, assess, and correct the deficiencies.~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals~~, and did not identify, assess, and correct the deficiencies.~~. (5.4) OR The Responsible Entity has implemented	physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies. (5.2)~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies. (5.3)~~. (5.3)	physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies.~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies. (5.3)~~. (5.3)	determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies. (5.2)~~. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals~~, and did not identify, assess, and correct the deficiencies.~~. (5.5) OR			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances~~, and did not identify, assess, and correct the deficiencies. (5.5)~~. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/2015	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

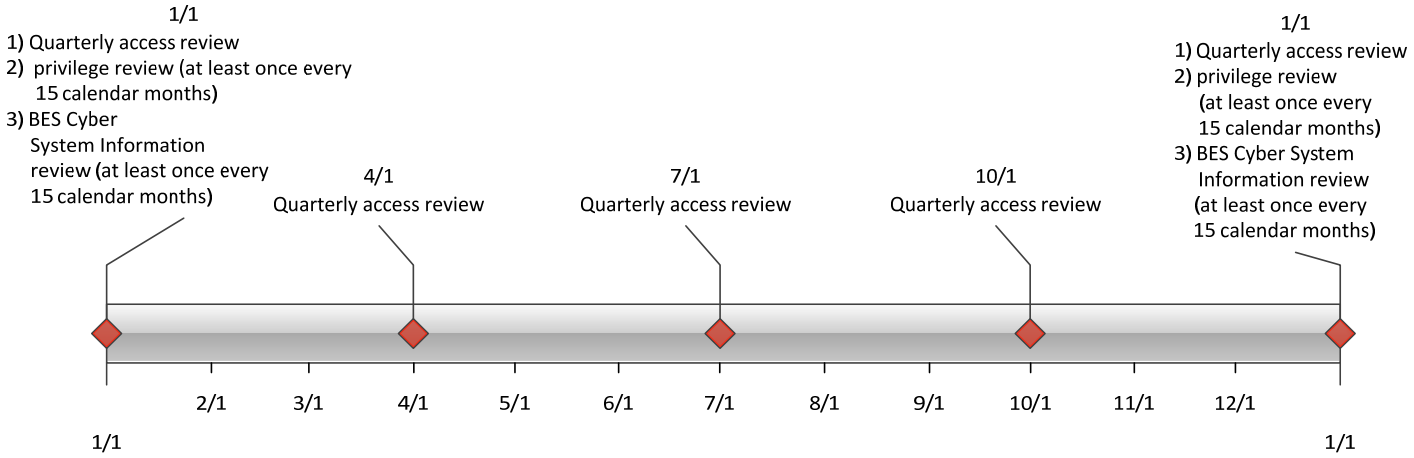
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts~~ text boxes were embedded within the standard~~.~~ to explain the rationale for various parts of the standard. Upon BOT approval, ~~that information~~the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such

authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

~~**Summary of Changes:** Reformatted into table structure.~~

~~**Reference to prior version:** (Part 1.1) CIP-004-4, R1~~

~~**Change Rationale:** (Part 1.1)~~

~~*Changed to remove the need to ensure or prove everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*~~

~~*Moved example mechanisms to guidance.*~~

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

~~Based on their role, some personnel may not require training on all topics.~~

~~**Summary of Changes:**~~

~~1. Addition of specific role training for:~~

- ~~The visitor control program~~
- ~~Electronic interconnectivity supporting the operation and control of BES Cyber Systems~~
- ~~Storage media as part of the handling of BES Cyber Systems information~~

~~2. Change references from Critical Cyber Assets to BES Cyber Systems.~~

~~**Reference to prior version:** (Part 2.1) CIP004-4, R2.2.1~~

~~**Change Rationale:** (Part 2.1)~~

~~*Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core*~~

~~*training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*~~

~~**Reference to prior version:** (Part 2.2) CIP004-4, R2.1~~

~~**Change Rationale:** (Part 2.2)~~

~~*Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*~~

~~**Reference to prior version:** (Part 2.3) CIP004-4, R2.3~~

~~**Change Rationale:** (Part 2.3)~~

~~*Updated to replace "annually" with "once every 15 calendar months."*~~

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

~~**Summary of Changes:** Specify that the seven-year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.~~

~~**Reference to prior version:** (Part 3.1) CIP004-4, R3.1~~

~~**Change Rationale:** (Part 3.1)~~

~~*Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*~~

~~**Reference to prior version:** (Part 3.2) CIP004-4, R3.1~~

~~**Change Rationale:** (Part 3.2)~~

~~*Specify that the seven-year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*~~

~~**Reference to prior version:** (Part 3.3) New~~

~~**Change Rationale:** (Part 3.3)~~

~~*There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.*~~

~~**Reference to prior version:** (Part 3.4) CIP-004-4, R3.3~~

~~**Change Rationale:** (Part 3.4)~~

~~*Separated into its own table item.*~~

~~**Reference to prior version:** (Part 3.5) CIP-004-3, R3, R3.3~~

~~**Change Rationale:** (Part 3.5)~~

~~*Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3*~~

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-~~5~~6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-~~5~~6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

~~**Summary of Changes:** The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.~~

~~**Reference to prior version:** (Part 4.1) CIP-003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1~~

~~**Change Rationale:** (Part 4.1)~~

~~Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*~~

~~**Reference to prior version:** (Part 4.2) CIP-004-4, R4.1~~

~~**Change Rationale:** (Part 4.2)~~

~~*Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4,~~ ~~**Requirement** *R*~~*4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

~~**Summary of Changes:** FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).~~

~~As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."~~

~~**Reference to prior version:** (Part 5.1) CIP-004-4, R4.2~~

~~**Change Rationale:** (Part 5.1)~~

~~*The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* **to require immediate revocation** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*~~

~~**Reference to prior version:** (Part 5.2) CIP-004-4, R4.2~~

~~**Change Rationale:** (Part 5.2)~~

~~*FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in*~~

~~*accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*~~

~~**Reference to prior version:** (Part 5.3) New~~

~~**Change Rationale:** (Part 5.3)~~

~~*FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*~~

~~**Reference to prior version:** (Part 5.4) New~~

~~**Change Rationale:** (Part 5.4)~~

~~*FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*~~

~~**Reference to prior version:** (Part 5.5) CIP-007-4, R5.2.3~~

~~**Change Rationale:** (Part 5.5)~~

~~*To provide clarification of expected actions in managing the passwords.*~~

~~Version History~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~1/16/06~~	~~R3.2 — Change "Control Center" to "control center."~~	~~3/24/06~~

~~2~~	~~9/30/09~~	~~Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a responsible entity.~~ ~~Rewording of Effective Date.~~ ~~Changed compliance monitor to Compliance Enforcement Authority.~~	
~~3~~	~~12/16/09~~	~~Updated version number from 2 to 3~~ ~~Approved by the NERC Board of Trustees.~~	
~~3~~	~~3/31/10~~	~~Approved by FERC.~~	
~~4~~	~~12/30/10~~	~~Modified to add specific criteria for Critical Asset identification.~~	~~Update~~
~~4~~	~~1/24/11~~	~~Approved by the NERC Board of Trustees.~~	~~Update~~
~~5~~	~~11/26/12~~	~~Adopted by the NERC Board of Trustees.~~	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~
~~5.1~~	~~9/30/13~~	~~Modified two VSLs in R4.~~	~~Errata~~
~~5.1~~	~~11/22/13~~	~~FERC Order issued approving CIP-004-5.1. (Order becomes effective on 2/3/14.)~~	
~~5.1~~	~~4/2/14~~	~~Address FERC Order 791 directive to modify Requirement R4 VRF and VSLs~~	~~R4 – VRF and VSLs~~

Reliability Standard CIP-006-6 Clean and Redline

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-006-6.

6. Background:

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Medium**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of	

Version	Date	Action	Change Tracking
		Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable

communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-~~5~~6

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum –** CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

See Implementation Plan for CIP-006-6.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires, which require the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their its documented

processes, but ~~they~~it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept

from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented physical security ~~plans~~plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~5~~6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~5~~6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~5~~6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-~~5~~6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-~~5~~6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-~~5~~6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~5~~6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-~~5~~6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented visitor control ~~programs~~program(s) that include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-~~5~~6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~(""~~ (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

- ~~Complaint~~

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	~~The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8)~~ ~~OR~~ ~~The Responsible Entity has a~~	~~The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and~~	~~The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity~~	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR ~~The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified~~	~~identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)~~ N/A	~~has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the~~	~~documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1)~~ ~~OR~~ The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~deficiencies but did not assess or correct the deficiencies. (1.9)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)~~ N/A		~~deficiencies. (1.6)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)~~ N/A	~~correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2)~~ ~~OR~~ The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR ~~The Responsible Entity documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)~~ ~~OR~~ The Responsible Entity does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~identify, assess, or correct the deficiencies. (1.4)~~ ~~OR~~ The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical ~~security~~Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	~~The Responsible Entity included a visitor control program that requires logging of each~~	~~The Responsible Entity included a visitor control program that requires continuous~~	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at~~	~~escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)~~ N/A	requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)~~N/A		
R3	**Long Term Planning**	**Medium**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity ~~has~~did not ~~documented and implemented~~document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of	

Version	Date	Action	Change Tracking
		Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus ~~is~~of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances ~~this~~a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, ~~a sole perimeter's~~ controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person ~~they are~~the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.~~7~~6 and 1.~~8~~7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts~~ text boxes were embedded within the standard~~.~~ to explain the rationale for various parts of the standard. Upon BOT approval, ~~that information~~the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.~~7~~6 and 1.~~8~~7 beyond what is already required for the PSP.

~~**Summary of Changes:** The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.~~

~~Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.~~

~~Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.~~

~~**Reference to prior version:** (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*~~

~~**Change Rationale:** (Part 1.1)~~

~~*To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.*~~

~~**Reference to prior version:** (Part 1.2) CIP006-4c, R3 & R4~~
~~**Change Rationale:** (Part 1.2)~~

~~*This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*~~

~~**Reference to prior version:** (Part 1.3) CIP006-4c, R3 & R4~~

~~**Change Rationale:** (Part 1.3)~~

~~*The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.*~~

~~*Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.*~~
~~*FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*~~

~~**Reference to prior version:** (Part 1.4) CIP006-4c, R5~~

~~**Change Rationale:** (Part 1.4)~~

~~*Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*~~

~~**Reference to prior version:** (Part 1.5) CIP006-4c, R5~~

~~**Change Rationale:** (Part 1.5)~~

~~*Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*~~

~~**Reference to prior version:** (Part 1.6) CIP006-4c, R5~~

~~**Change Rationale:** (Part 1.6)~~

~~*Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*~~

~~**Reference to prior version:** (Part 1.7) CIP006-4c, R5~~

~~**Change Rationale:** (Part 1.7)~~

~~*Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*~~

~~**Reference to prior version:** (Part 1.8) CIP-006-4c, R6~~

~~**Change Rationale:** (Part 1.8)~~

~~*CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.*~~

~~*Examples of logging methods have been moved to the Guidelines and Technical Basis section.*~~

~~**Reference to prior version:** (Part 1.9) CIP-006-4c, R7~~

~~**Change Rationale:** (Part 1.9)~~

~~*No change.*~~

~~**Rationale for R2:**~~

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance	

Version	Date	Action	Change Tracking
		elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5. (Order becomes effective on 2/3/14.)	
5	4/2/14	Address directive in FERC Order 791 to modify VRF in Requirement R3	VRF – R3

Reliability Standard CIP-007-6 Clean and Redline

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-007-6.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-6 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

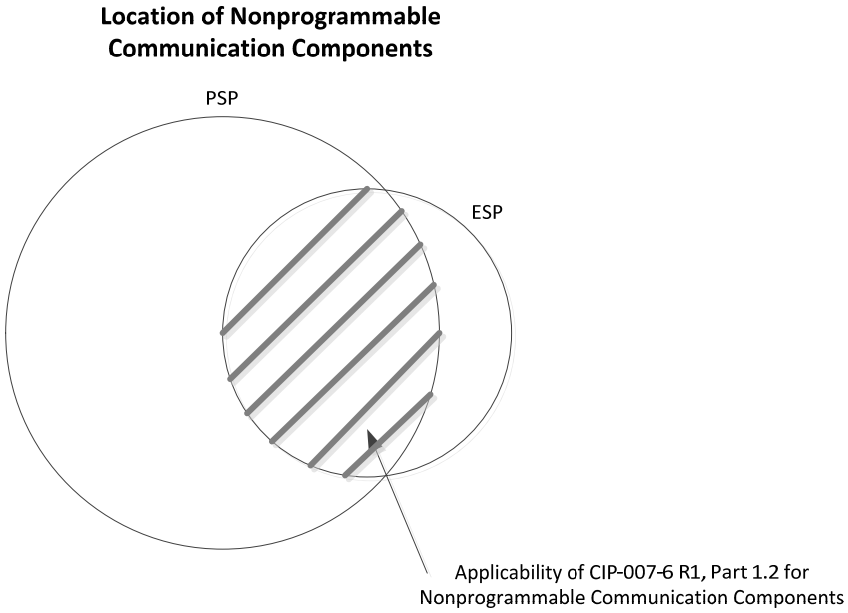
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-

time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-~~5~~6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the ~~BES.~~Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. ~~5.~~ Effective Dates:

~~1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-007-6.

6. Background:

Standard CIP-007-~~5~~ exists as part of a suite of CIP Standards related to cyber security~~.~~ ~~CIP-002-5~~, which requires the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~].~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System.~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~5~~6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable media.~~Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~5~~6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-~~5~~6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~5~~6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~("~~" (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Violation Investigations

Self-Reporting

~~• Complaint~~

Complaints

1.4. Additional Compliance Information:

None

~~D. Regional Variances~~

~~None.~~

~~E. Interpretations~~

~~None.~~

~~F. Associated Documents~~

~~None.~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable media and has identified deficiencies but did not assess or correct the deficiencies.~~Removable Media. (1.2) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical~~	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (1.1) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5 Table R1 and has identified deficiencies but did not assess or correct the deficiencies.~~6 Table R1. (R1) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)~~	~~determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)~~	~~the deficiencies. (R1)~~
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets ~~and has identified deficiencies but did not~~	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets ~~and has identified~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5 Table R2 and has identified deficiencies but did not assess or correct the~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but less than 50 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies.~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for~~	~~assess or correct the deficiencies.~~. (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	~~deficiencies but did not assess or correct the deficiencies.~~. (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and implemented one	~~deficiencies.~~6 Table R2. (R2) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2)~~ OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50	applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies.~~ (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days~~	or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies.~~ (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did~~	or installing cyber security patches for applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies.~~ (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days of the evaluation completion ~~and has identified deficiencies but did not assess or correct the deficiencies.~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35~~	~~of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion ~~and has identified deficiencies~~	~~not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	~~correct the deficiencies. (2.1)~~ OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate ~~and has identified deficiencies but did not assess or correct the deficiencies.~~. (2.4) ~~OR~~ ~~The Responsible Entity documented a mitigation plan~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~but did not assess or correct the deficiencies.~~ (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or~~	plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies.~~ (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable~~	~~for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4)~~ OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan~~ and has identified deficiencies but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~correct the deficiencies. (2.3)~~	~~patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~not assess or correct the deficiencies.~~. (2.4) ~~OR~~ ~~The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)~~
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns	The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				are used, the Responsible Entity did not address testing the signatures or patterns ~~and has identified deficiencies but did not assess or correct the deficiencies.~~. (3.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)~~	malicious code prevention but did not mitigate the threat of detected malicious code~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (3.2) OR ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2)~~	that included the applicable items in CIP-007-~~5 Table R3 and has identified deficiencies but did not assess or correct the deficiencies. (R3)~~6 Table R3. (R3). ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify, assess, or correct the deficiencies. (R3)~~ OR The Responsible Entity has implemented one

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~OR~~ The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections ~~and has identified deficiencies but did not assess or correct the deficiencies. (3.3)~~ ~~OR~~ ~~The Responsible Entity has implemented one or more documented~~	or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code ~~and has identified deficiencies but did not assess or correct the deficiencies.~~. (3.1) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)~~. (3.3).	~~did not identify, assess, or correct the deficiencies. (3.1)~~
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5 Table R4 and has identified deficiencies but did not assess or correct the deficiencies.~~6 Table R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			days but missed an interval and completed the review within 22 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (4.4) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an~~	within 30 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (4.4) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or~~	not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 ~~and has identified deficiencies but did not assess or correct the deficiencies.~~. (4.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the~~	~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)~~ OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)~~	~~correct the deficiencies. (4.4)~~	~~required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2)~~ OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days~~ and has identified deficiencies but did~~	types of events described in 4.1.1 through 4.1.3~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (4.1) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies.~~ (4.3) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3)~~ OR	~~the deficiencies. (4.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals ~~and has identified deficiencies but did not assess or correct the deficiencies. (4.4)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented one~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)~~. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~*5 Table R5 and has identified deficiencies but did*~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for~~	an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change ~~and has identified deficiencies but did not assess or correct the deficiencies.~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change~~	inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s~~) and has identified deficiencies but did not assess or correct the deficiencies.~~). (5.2) OR ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled~~	~~not assess or correct the deficiencies.~~6 Table R5. (R5) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5)~~ OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~and did not identify, assess, or correct the deficiencies. (5.6)~~	~~default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2)~~ ~~OR~~ The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts ~~and has identified deficiencies but did~~	technically feasible, does not have a method(s) to enforce authentication of interactive user access~~ and has identified deficiencies but did not assess or correct the deficiencies.~~ (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (5.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)~~ OR The Responsible Entity has implemented one or more	access~~ and did not identify, assess, or correct the deficiencies.~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (5.4) ~~OR~~ ~~The Responsible Entity has implemented one~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for	~~or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4)~~ OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2~~ and did not identify, assess, or correct the deficiencies.~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an	password parameters described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies.~~. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change ~~and has identified deficiencies but did not assess or correct the deficiencies.~~ (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally~~	~~and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5)~~ OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change ~~and has identified deficiencies but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~not assess or correct the deficiencies. (5.6)~~ ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~correct the deficiencies.~~ (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts ~~and has identified deficiencies but did not assess or~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~correct the deficiencies. (5.7)~~ ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7).~~ (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

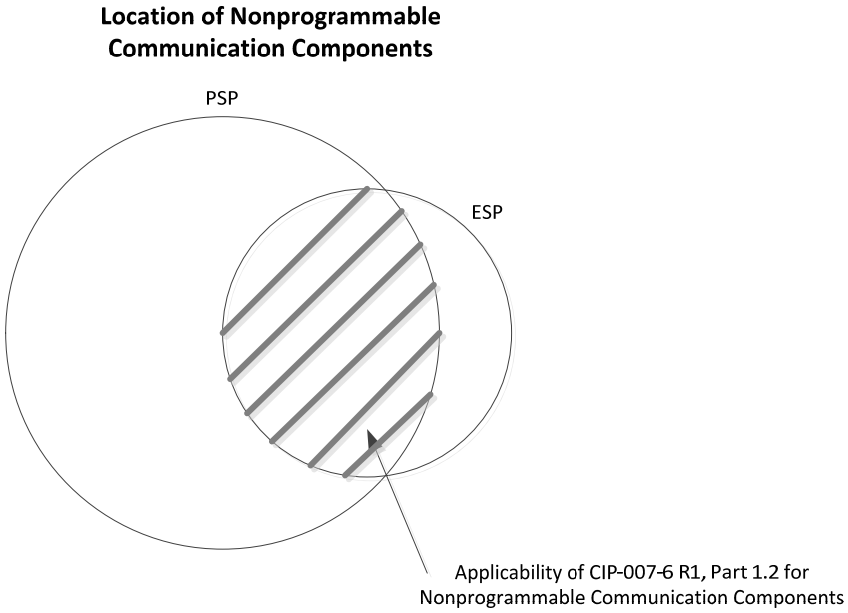
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense ~~are~~is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. ~~Stand alone~~Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, ~~portable storage media policies,~~ Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of ~~removable media~~Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-

time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc~~).~~.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts~~ text boxes were embedded within the standard~~.~~ to explain the rationale for various parts of the standard. Upon BOT approval, ~~that information~~the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

~~**Summary of Changes:** Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.~~

~~**Reference to prior version:** (Part 1.1) CIP-007-4, R2.1 and R2.2~~

~~**Change Rationale:** (Part 1.1)~~

~~*The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*~~

~~**Reference to prior version:** (Part 1.2) New~~

~~**Change Rationale:** (Part 1.2)~~

~~*On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*~~

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

~~The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.~~

~~**Summary of Changes:** The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.~~

~~**Reference to prior version:** (Part 2.1) CIP-007, R3~~

~~**Change Rationale:** (Part 2.1)~~

~~*The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*~~

~~**Reference to prior version:** (Part 2.2) CIP-007, R3.1~~

~~**Change Rationale:** (Part 2.2)~~

~~*Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 35-day time frame.*~~

~~**Reference to prior version:** (Part 2.3) CIP-007, R3.2~~

~~**Change Rationale:** (Part 2.3)~~

~~*The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*~~

~~**Reference to prior version:** (Part 2.4) CIP-007, R3.2~~

~~**Change Rationale:** (Part 2.4)~~

~~*Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.*~~

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

~~**Summary of Changes:** In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.~~

~~Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"~~

~~In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.~~

~~**Reference to prior version:** (Part 3.1) CIP-007-4, R4; CIP-007-4, R4.1~~

~~**Change Rationale:** (Part 3.1)~~

~~*See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*~~

~~**Reference to prior version:** (Part 3.2) *CIP-007-4, R4; CIP-007-4, R4.1*~~
~~**Change Rationale:** (Part 3.2)~~

~~*See the Summary of Changes.*~~

~~**Reference to prior version:** (Part 3.3) CIP-007-4, R4; CIP-007-4, R4.2~~

~~**Change Rationale:** (Part 3.3)~~

~~**Requirement** *essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.*~~

Rationale for Requirement R4:

~~**Rationale for R4:**~~ Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

~~**Summary of Changes:** Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."~~

~~The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.~~

~~In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.~~

~~**Reference to prior version:** (Part 4.1) CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3~~

~~**Change Rationale:** (Part 4.1)~~

~~*This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4* **Requirement** *R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*~~

~~**Reference to prior version:** (Part 4.2) CIP-005-4, R3.2; CIP-007-4, R6.2~~

~~**Change Rationale:** (Part 4.2)~~

~~*This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.*~~

~~**Reference to prior version:** (Part 4.3) CIP-005-4, R3.2; CIP-007-4, R6.4~~

~~**Change Rationale:** (Part 4.3)~~

~~*No substantive change.*~~

~~**Reference to prior version:** (Part 4.4) CIP-005-4, R3.2; CIP-007-4, R6.5~~

~~**Change Rationale:** (Part 4.4)~~

~~*Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.*~~

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to

make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts

for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

~~Summary of Changes (From R5):~~

~~CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.~~

~~Reference to prior version:~~ ~~(Part 5.1) CIP-007-4, R5~~

~~Change Rationale:~~ ~~(Part 5.1)~~

~~*The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*~~

~~Reference to prior version:~~ ~~(Part 5.2) CIP-007-4, R5.2 and R5.2.1~~

~~Change Rationale:~~ ~~(Part 5.2)~~

~~*CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*~~

~~Reference to prior version:~~ ~~(Part 5.3) CIP-007-4, R5.2.2~~

~~Change Rationale:~~ ~~(Part 5.3)~~

~~*No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*~~

~~Reference to prior version:~~ ~~(Part 5.4) CIP-007-4, R5.2.1~~

~~Change Rationale:~~ ~~(Part 5.4)~~

~~*The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of*~~

having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.

Reference to prior version: (Part 5.5) CIP-007-4, R5.3

Change Rationale: (Part 5.5)

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.

Reference to prior version: (Part 5.6) CIP-007-4, R5.3.3

Change Rationale: (Part 5.6)

**This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

Reference to prior version: (Part 5.7) *New Requirement*

Change Rationale: (Part 5.7)

Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance	

		~~with the latest guidelines for developing compliance elements of standards.~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a responsible entity.~~ ~~Rewording of Effective Date.~~ ~~Changed compliance monitor to Compliance Enforcement Authority.~~	
~~3~~	~~12/16/09~~	~~Updated version number from -2 to -3~~ ~~Approved by the NERC Board of Trustees.~~	
~~3~~	~~3/31/10~~	~~Approved by FERC.~~	
~~4~~	~~12/30/10~~	~~Modified to add specific criteria for Critical Asset identification.~~	~~Update~~
~~4~~	~~1/24/11~~	~~Approved by the NERC Board of Trustees.~~	~~Update~~
~~5~~	~~11/26/12~~	~~Adopted by the NERC Board of Trustees.~~	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~
~~5~~	~~11/22/13~~	~~FERC Order issued approving CIP-007-5. (Order becomes effective on 2/3/14.)~~	

Reliability Standard CIP-009-6 Clean and Redline

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-009-6.

6. Background:

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show

documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

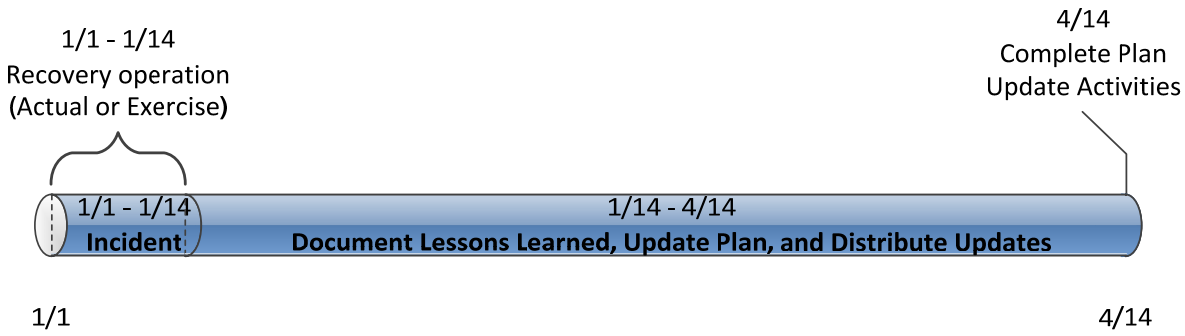


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

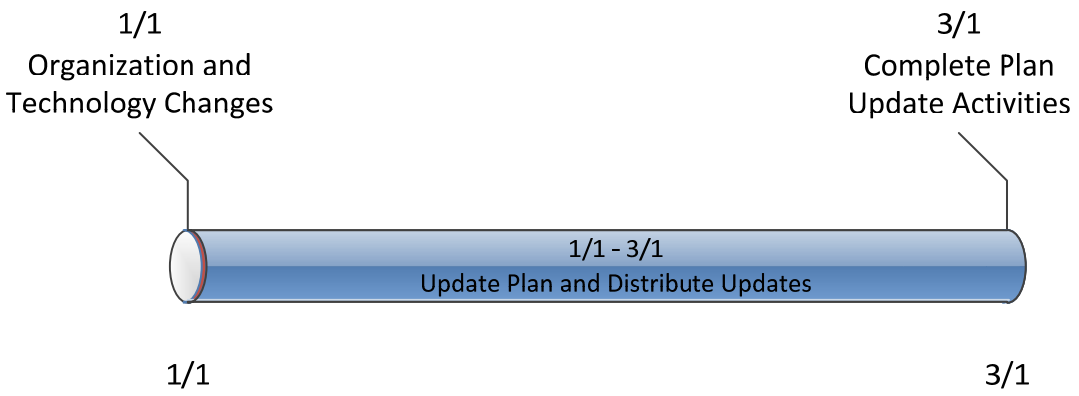


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-~~5~~6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. ~~5.~~ Effective Dates:

~~1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-009-6.

6. Background:

Standard CIP-009~~-5~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~.~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery ~~plans~~plan(s) that collectively include each of the applicable requirement parts in *CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications*.

CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery ~~plans~~plan(s) in accordance with each of the applicable requirement parts in *CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~("~~" (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

~~• Complaint~~

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected.~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests~~, and~~	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected.~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests~~, and when tested, any~~	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected.~~ (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests~~, and~~	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~when tested, any deficiencies were identified, assessed, and corrected.~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)~~. (2.3)	~~deficiencies were identified, assessed, and corrected.~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)~~. (2.3)	~~when tested, any deficiencies were identified, assessed, and corrected.~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)~~ . (2.3)	~~OR~~ The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR ~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~OR~~ ~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)~~ ~~OR~~ The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)~~
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power ~~plants' facilities~~plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1~~Figure 1~~, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

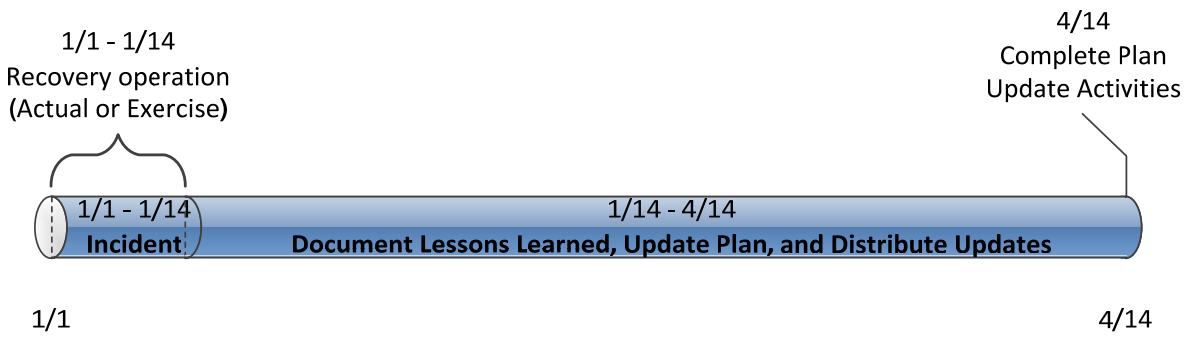


Figure 1: CIP-009-~~5~~6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2~~Figure 2~~, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

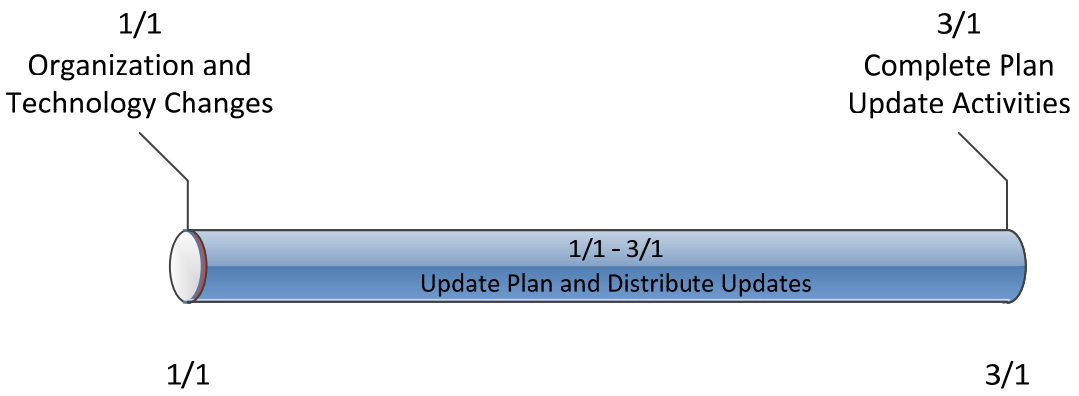


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts~~ text boxes were embedded within the standard~~.~~ to explain the rationale for various parts of the standard. Upon BOT approval, ~~that information~~the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

~~**Summary of Changes:** Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.~~

~~**Reference to prior version:** (Part 1.1) CIP-009, R1.1~~

~~**Change Description and Justification:** (Part 1.1)~~

~~*Minor wording changes; essentially unchanged.*~~

~~**Reference to prior version:** (Part 1.2) CIP-009, R1.2~~

~~**Change Description and Justification:** (Part 1.2)~~

~~*Minor wording changes; essentially unchanged.*~~

~~**Reference to prior version:** (Part 1.3) CIP-009, R4~~

~~**Change Description and Justification:** (Part 1.3)~~

~~*Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.*~~

~~**Reference to prior version:** (Part 1.4) New Requirement~~

~~**Change Description and Justification:** (Part 1.4)~~

~~*Addresses FERC Order Section 739 and 748.*~~

~~**Reference to prior version:** (Part 1.5) New Requirement~~

~~**Change Description and Justification:** (Part 1.5)~~

~~*Added requirement to address FERC Order No. 706, Paragraph 706.*~~

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

~~**Summary of Changes.** Added operational testing for recovery of BES Cyber Systems.~~

~~**Reference to prior version:** (Part 2.1) CIP-009, R2~~

~~**Change Description and Justification:** (Part 2.1)~~

~~*Minor wording change; essentially unchanged.*~~

~~**Reference to prior version:** (Part 2.2) CIP-009, R5~~

~~**Change Description and Justification:** (Part 2.2)~~

~~*Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.*~~

~~**Reference to prior version:** (Part 2.3) CIP-009, R2~~

~~**Change Description and Justification:** (Part 2.3)~~

~~*Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.*~~

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

~~**Summary of Changes:** Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.~~

~~**Reference to prior version:** (Part 3.1) CIP-009, R1 and R3~~

~~**Change Description and Justification:** (Part 3.1)~~

~~*Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.*~~

~~**Reference to prior version:** (Part 3.2) New Requirement~~

~~**Change Description and Justification:** (Part 3.2)~~

~~*Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.*~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5. (Order becomes effective on 2/3/14.)	
5	4/2/14	Address directive in FERC Order 791 to modify VSLs in Requirement R3	VSLs – R3

Reliability Standard CIP-010-2 Clean and Redline

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show

documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			manage its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for	implement the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to	authorize its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible	Removable Media according to CIP-010-2, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)	CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1,	Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Sections 2.1, 2.2, and 2.3. (R4)	R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Guideline and Technical Basis (attached).

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

CIP-010-2 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-2 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;

- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those

types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update

of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.

- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-~~1~~2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the ~~BES.~~Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~1. **24 Months Minimum –** CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-010-2.

6. Background:

Standard CIP-010~~-1~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~]~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System.~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS~~) –~~) –** Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS~~) –~~) –** Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R3– Vulnerability Assessments. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment~~;~~; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~1~~2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~1~~2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process:

1.1 Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~("~~" (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2 Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

~~Complaint~~Complaints

1.4 Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline~~	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR ~~The Responsible Entity has documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~	~~but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be~~	~~items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~	~~implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify,~~	~~impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the~~	~~The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify,~~	~~assess, and correct the deficiencies. (1.1)~~ ~~OR~~ The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~assess, or correct the deficiencies in the verification documentation. (1.4.3)~~	~~determination of affected security controls. (1.4.1)~~	~~assess, or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update baseline configurations~~	OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess,~~	not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~or correct the deficiencies. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the~~	document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~the deficiencies. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the deficiencies. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment,~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)~~	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. ~~(2.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~or correct the deficiencies. (2.1)~~(2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			manage its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for	implement the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to	authorize its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible	Removable Media according to CIP-010-2, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)	CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1,	Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Sections 2.1, 2.2, and 2.3. (R4)	R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~

Guideline and Technical Basis (attached).

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

CIP-010-2 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-2 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-~~5~~6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-~~5~~6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 ~~R1~~Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;

- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those

types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update

of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.

- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts~~ text boxes were embedded within the standard~~.~~ to explain the rationale for various parts of the standard. Upon BOT approval, ~~that information~~the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

~~**Reference to prior version:** (Part 1.1) New Requirement~~

~~**Change Rationale:** (Part 1.1)~~

~~*The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*~~

~~**Reference to prior version:** (Part 1.2) CIP-007-3, R9; CIP-003-3, R6~~

~~**Change Rationale:** (Part 1.2)~~

~~*The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*~~

~~**Reference to prior version:** (Part 1.3) CIP-007-3, R9; CIP-005-3, R5~~

~~**Change Rationale:** (Part 1.3)~~

~~*Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*~~

~~**Reference to prior version:** (Part 1.4) CIP-007-3, R1~~

~~**Change Rationale:** (Part 1.4)~~

~~*The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*~~

~~**Reference to prior version:** (Part 1.5) CIP-007-3, R1~~

~~**Change Rationale:** (Part 1.5)~~

~~*This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.*~~

~~*This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*~~

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

~~**Reference to prior version:** (Part 2.1) New Requirement~~

~~**Change Rationale:** (Part 2.1)~~

~~*The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.*~~

~~*This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.*~~

~~*Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*~~

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

~~**Reference to prior version:** (Part 3.1) CIP-005-4, R4; CIP-007-4, R8~~

~~**Change Rationale:** (Part 3.1)~~

~~*As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*~~

~~**Reference to prior version:** (Part 3.2) New Requirement~~

~~**Change Rationale:** (Part 3.2)~~

~~*FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*~~

~~*As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*~~

~~**Reference to prior version:** (Part 3.3) New Requirement~~

~~**Change Rationale:** (Part 3.3)~~
~~*FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*~~

~~**Reference to prior version:** (Part 3.4) CIP-005-3, R4.5; CIP-007-3, R8.4~~

~~**Change Rationale:** (Part 3.4)~~
~~*Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*~~

~~Version History~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~

~~1~~	~~11/26/12~~	~~Adopted by the NERC Board of Trustees.~~	~~Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.~~
~~1~~	~~11/22/13~~	~~FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)~~	

Rationale for Requirement R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Reliability Standard CIP-011-2 Clean and Redline

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-011-2.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Guideline and Technical Basis (attached).

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:
The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~1~~2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the ~~BES.~~Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~1. **24 Months Minimum** – CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

See Implementation Plan for CIP-011-2.

6. Background:

Standard CIP-011~~-1~~ exists as part of a suite of CIP Standards related to cyber security~~.~~ ~~CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~.~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any

particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table~~. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities~~.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System.~~BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA~~)~~)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~1~~2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~1~~2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~1~~2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

R2. Each Responsible Entity shall implement one or more documented ~~processes~~process(es) that collectively include the applicable requirement parts in *CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~("~~" (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance ~~Audit~~Audits
- Self-~~Certification~~Certifications
- Spot Checking
- Compliance ~~Investigation~~Violation Investigations
- Self-Reporting
- ~~Complaint~~
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify,~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~assess, or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~but did not identify, assess, or correct the deficiencies. (1.2)~~N/A	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~

Guideline and Technical Basis (attached).

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the ~~responsible entity~~Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale:

During ~~the~~ development of this standard, ~~references to prior versions of the CIP standards and rationale for the requirements and their parts~~ text boxes were embedded within the standard~~.~~ to explain the rationale for various parts of the standard. Upon BOT approval, ~~that information~~the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:
The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

~~**Summary of Changes:** CIP-003-4 R4, R4.2, and R 4.3 have been moved to CIP-011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.~~

~~**Reference to prior version:** (Part 1.1) CIP-003-3, R4; CIP-003-3, R4.2~~

~~**Change Rationale:** (Part 1.1)~~

~~*The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (e.g., confidential, public, internal use only, etc.) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*~~

~~**Reference to prior version:** (Part 1.2) CIP-003-3, R4~~

~~**Change Rationale:** (Part 1.2)~~

~~*The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.*~~

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

~~**Reference to prior version:** (Part 2.1) CIP-007-3, R7.2~~

~~**Change Rationale:** (Part 2.1)~~

~~*Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*~~

~~**Reference to prior version:** (Part 2.2) CIP-007-3, R7.1~~

~~**Change Rationale:** (Part 2.2)~~

~~*Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*~~

~~*The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*~~

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	

Definition of Terms Used in Standards

Definitions of Terms Used in Standards

This section includes new and modified defined terms used in the proposed standards. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New definitions listed below become approved when the proposed standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

Removable Media: Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset: A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to,

Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Definitions of Terms Used in Standards

This section includes revised terms used in the proposed standards. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. Revised definitions listed below become approved when the proposed standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

Redline to Last Approved

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. ~~(A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)~~

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. ~~A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.~~

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

January 23, 2015

This Implementation Plan for the Reliability Standards developed as part of Project 2014-02 CIP Version 5 Revisions replaces the Implementation Plan for the versions of those CIP Reliability Standards adopted by the NERC Board of Trustees on November 13, 2014.

Requested Approvals[+]

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel & Training
- CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems[*]
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems[*]
- CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-2 — Cyber Security — Information Protection

[+] During development, Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 were balloted as CIP-003-7, CIP-004-7, CIP-007-7, CIP-10-3, and CIP-011-3. Because these Reliability Standards replace versions of these Reliability Standards adopted by the Board in November 2014 using version numbers -6 and -2, which have not been filed with applicable governmental authorities, the version numbers will revert back to -6 and -2 for purposes of Board adoption and filing with applicable governmental authorities.

[*] The NERC Board of Trustees adopted Reliability Standards CIP-006-6 and CIP-009-6, and an associated implementation plan, on November 13, 2014. While these Reliability Standards are not being presented again for ballot or Board adoption, they are included herein for ease of reference and to provide a single implementation plan that contains all of the Reliability Standards adopted as part of Project 2014-02 CIP Version 5 Revisions.

Requested Board Withdrawals

NERC is requesting that the Board withdraw the following CIP Reliability Standards adopted by the Board of Trustees on November 13, 2014 and replace them with the revised versions of these CIP Reliability Standards presented to the Board on February 12, 2015:

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel & Training
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements**

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5.1 — Cyber Security — Personnel & Training
- CIP-006-5 — Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

** The NERC Board of Trustees approved the retirement of Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1 on November 13, 2014. While these Reliability Standards are not being presented again for retirement, they are included herein for ease of reference and to provide a single implementation plan that contains all of the requested Board actions as part of Project 2014-02 CIP Version 5 Revisions.

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Transient Cyber Asset	A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Low Impact BES Cyber System Electronic Access Point (LEAP)	A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.
Low Impact External Routable Connectivity (LERC)	Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The compliance date for those particular sections represents the date that entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-6 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-003-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Requirement R2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 1

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 2 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 3

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 4

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

2. CIP-004-6 — Cyber Security — Personnel & Training

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable

governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems[1]

   Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-006-6, Requirement R1, Part 1.10

   For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-6 — Cyber Security — Systems Security Management

   Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the

[1] The NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with high and medium impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems[2]

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

[2] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

Compliance Date for CIP-010-2, Requirement R4

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

7. CIP-011-2 — Cyber Security — Information Protection

   Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

   The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the compliance date for Reliability Standard CIP-010-2, Requirement R4, as applicable in the relevant jurisdiction.

   The new and modified NERC Glossary Terms Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity shall become effective on the compliance date for Reliability Standard CIP-003-6, Requirement R2, as applicable in the relevant jurisdiction.

9. Standards for Retirement[3]

   CIP-003-5 shall retire at midnight of the day immediately prior to the effective date of CIP-003-6 in the particular jurisdiction in which the new standard is becoming effective.

   CIP-004-5.1 shall retire at midnight of the day immediately prior to the effective date of CIP-004-6 in the particular jurisdiction in which the new standard is becoming effective.

[3] As noted above, the NERC Board retired these Reliability Standards in November 2014. Therefore, they are not being presented again for retirement but are included in this implementation plan for ease of reference.

CIP-006-5 shall retire at midnight of the day immediately prior to the effective date of CIP-006-6 in the particular jurisdiction in which the new standard is becoming effective.[4]

CIP-007-5 shall retire at midnight of the day immediately prior to the effective date of CIP-007-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-009-5 shall retire at midnight of the day immediately prior to the effective date of CIP-009-6 in the particular jurisdiction in which the new standard is becoming effective.[5]

CIP-010-1 shall retire at midnight of the day immediately prior to the effective date of CIP-010-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-011-1 shall retire at midnight of the day immediately prior to the effective date of CIP-011-2 in the particular jurisdiction in which the new standard is becoming effective.

10. Standards for Withdrawal

    The withdrawal of Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 that were adopted by the Board in November 2014 shall become effective immediately upon Board adoption of the replacement Reliability Standards.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[6] (Version 5 Plan) remain the same:

[4] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.
[5] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.
[6] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Exhibit C

Order No. 672 Criteria

EXHIBIT C

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standards meet or exceed the criteria.

1. **Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[2]**

The proposed Reliability Standards achieve the specific reliability goals of requiring entities to implement cybersecurity controls for (1) low impact BES Cyber Systems, (2) transient electronic devices, and (3) non-programmable components of communication networks, consistent with the Commissions directives in Order No. 791. The proposed Reliability Standards articulate clear security objectives for each of the areas and provide responsible entities the flexibility to implement whatever combination of security controls are necessary to meet those goals. The proposed Reliability Standards also remove compliance-oriented language from the CIP Reliability Standards to ensure that the performance obligations are clear and that compliance-related issues are addressed in NERC's Compliance Monitoring and Enforcement Program.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[2] Order No. 672 at PP 321, 324.

2. Proposed Reliability Standards must be applicable only to users, owners and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.[3]

The proposed Reliability Standards are clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed Reliability Standards clearly articulate the actions that applicable entities must take to comply with the standards.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.[4]

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for the proposed Reliability Standards comport with NERC and Commission guidelines related to their assignment, as discussed further in Exhibit E. The assignment of the severity level for each VSL is consistent with the corresponding requirement. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standards include clear and understandable consequences in accordance with Order No. 672.

4. A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner. [5]

The proposed Reliability Standards contain measures that support each requirement by clearly identifying what is required to demonstrate compliance. These measures help provide clarity regarding the manner in which the requirements will be enforced, and help ensure that the

---

3 Order No. 672 at PP 322, 325.

4 Order No. 672 at P 326.

5 Order No. 672 at P 327.

requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.

5. **Proposed Reliability Standards should achieve a reliability goal effectively and efficiently — but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[6]**

The proposed Reliability Standards achieve the reliability goals effectively and efficiently in accordance with Order No. 672. The proposed Reliability Standards clearly articulate the security objectives that applicable entities must meet and provides entities the flexibility to tailor their processes and plans required under the standard to best suit the needs of their organization.

6. **Proposed Reliability Standards cannot be "lowest common denominator," *i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[7]**

The proposed Reliability Standards do not reflect a "lowest common denominator" approach. To the contrary, the proposed Reliability Standards contains significant benefits for the Bulk-Power System. The requirements of the proposed Reliability Standards help ensure that entities provide an adequate level of protection against cyber-attacks to Bulk Electric System Facilities, systems, and equipment.

7. **Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns,**

---

6 Order No. 672 at P 328.

7 Order No. 672 at P 329-30.

and regional variations in market design if these affect the proposed Reliability Standard.[8]

The proposed Reliability Standards apply throughout North America and do not favor one geographic area or regional model.

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[9]

The proposed Reliability Standards have no undue negative impact on competition. The proposed Reliability Standards require the same performance by each applicable entity. The standards do not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

9. The implementation time for the proposed Reliability Standard is reasonable.[10]

The proposed effective dates for the proposed Reliability Standards are just and reasonable and appropriately balance the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must comply to develop and implement the necessary procedures and policies. The proposed implementation periods will allow applicable entities adequate time to meaningfully implement the requirements. The proposed effective dates are explained in the proposed Implementation Plan, attached as Exhibit B.

---

8 Order No. 672 at P 331.

9 Order No. 672 at P 332.

10 Order No. 672 at P 333.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[11]

The proposed Reliability Standards were developed in accordance with NERC's Commission-approved, ANSI- accredited processes for developing and approving Reliability Standards. Exhibit F includes a summary of the development proceedings, and details the processes followed to develop the proposed Reliability Standards. These processes included, among other things, comment and balloting periods. Additionally, all meetings of the drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum and exceeded the required ballot pool approval levels.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[12]

NERC has identified no competing public interests regarding the request for approval of the proposed Reliability Standards. No comments were received that indicated the proposed Reliability Standards conflicts with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.[13]

No other negative factors relevant to whether the proposed Reliability Standards are just and reasonable were identified.

---

11 Order No. 672 at P 334.

12 Order No. 672 at P 335.

13 Order No. 672 at P 323.

Exhibit D

Consideration of Directives

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791
January 23, 2015

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5.1, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
106	Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact	The SDT revised Requirements R1 and R2 of CIP-003-6 to include additional specificity regarding the processes that responsible entities must have for low impact BES Cyber Systems. In addition, the SDT developed objective criteria

[2] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 186, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.	surrounding the controls for some entities based on asset-type and routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category. To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility-site level. The SDT confined these revisions in CIP-003-6, Requirements R1 and R2 to the following areas: 1. **Cyber Security Policy:** R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan. 2. **Cyber Security Plan(s):** R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The cyber security plan must cover the 4 areas as specified in Attachment 1 of CIP-003-6: a. **Cyber Security Awareness:** Attachment 1, Section 1 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices. The SDT determined that adding intervals increases the auditability of the requirement part. b. **Physical Security Controls:** Attachment 1, Section 2 and its subparts require physical access controls to low impact BES Cyber Systems as well as Low Impact BES Cyber System Electronic Access Points (LEAP) used for controlling access as specified in Section 3. c. **Electronic Access Controls:** Attachment 1, Section 3 and its subparts address protections around Low Impact BES Cyber System External Routable Connectivity (LERC) and Dial-up Connectivity. d. **Cyber Security Incident Response:** Attachment 1, Section 4 and its subparts outline the criteria required to be in a Cyber Security Incident response plan.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing.
132	Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it	The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which requires a Transient Cyber Asset

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.	and Removable Media plan to provide higher assurance against the propagation of malware when connecting transient devices. The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition. The drafting team determined three distinct scenarios for entities to address in their plan(s) in which transient devices need specific protections: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Asset(s) managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media. For Transient Cyber Assets managed by the Responsible Entity, the SDT determined that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management. The controls for this scenario are

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		more specific and recognize the relatively higher frequency in which these devices will be used. In the scenario in which a party other than the Responsible Entity manages the Transient Cyber Assets, the required sections of the plan include those which an entity can verify at the point prior to connecting such as security patch management and malware prevention mechanisms. The security controls entities must apply to Removable Media have considerations for the type of device being protected and include authorization and scanning for malicious code. The Commission provided a list of security controls it expected NERC to consider for addressing transient devices. The consideration of each security section is described as follows: 1. **Device authorization as it relates to users and locations:** CIP-010-2 Requirement R4, Attachment 1 requires entities to authorize Transient Cyber Assets and Removable Media by user(s), location(s) and use prior to connecting them to the BES Cyber System. Transient Cyber Assets managed by another party do not have this authorization because the scenario is often single-use and the entity already conducts an inspection and mitigation of the device prior to connection.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		2. Software authorization: The SDT considered controls relating to software authorization but decided against including specific software as part of the authorization performance because such authorization did not contribute meaningfully to cyber security risk reduction. However, software authorization in the form of application whitelisting is provided as an option to mitigate malicious code. **3. Security patch management:** In CIP-010-2 R4, Attachment 1, both entity and vendor/contractor managed devices must have security patch management or other equivalent forms of mitigation to address security vulnerabilities in software. 4. **Malware prevention:** CIP-010-2 Requirement R4, Attachment 1 requires entities to have malware protection on the Transient Cyber Asset (for both entity- and vendor-managed Transient Cyber Assets) and for Removable Media prior to connection. 5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this control and determined this control best applies to entity-managed Transient Cyber Assets with the objective to mitigate the risk of unauthorized use. There are logistical challenges in applying this control to vendor-managed devices, in which the entity likely will

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		have had no control until immediately prior to use. Furthermore, additional guidance is necessary in CIP-011-2 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient devices. The objective to address the unauthorized release of BES Cyber System Information is sufficiently addressed with the requirements in CIP-011-2 to protect and securely handle BES Cyber System Information. 6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. high, medium, low impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-2 requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-2 Requirement R4.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." However, the scope of the requirements modifications as well as the existing requirements has more targeted components than the broad concept of

[3] *See infra* P 223.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		communication networks. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards. The decision to meet the directive without defining the term communication networks does not imply the absence of protection for communication networks components nor do the additional requirements associated with nonprogrammable components denote meaning to the term. Communication networking components associated with BES Cyber Systems and within an Electronic Security Perimeter have the same level of protection applied as the BES Cyber Assets themselves. Additionally, CIP-005-5 communication protections continue to apply at the Electronic Security Perimeter. The drafting team did not find an additional Glossary term useful in the currently applied communication networks protection.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to the CIP version 5 Standards.4 The Commission agrees that a pilot program will assist responsible entities by	NERC modified the VRF assignment for CIP-006-6, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	NERC modified the VRF assignment for CIP-004-6, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained sections. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-6, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language. 2. **VSLs for CIP-004-6, Requirement R4**. This standard includes requirements for personnel

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-6, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the timeframe contained in the VSLs from 90-210 days to 90-120 days.

Exhibit E

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02 - Cyber Security - Order No. 791 Identify, Assess, and Correct; Low Impact; Transient Devices; and Communication Networks Directives

Violation Risk Factor and Violation Severity Level Justifications

The tables in this document provide a working draft of the analysis and justification for each Violation Risk Factor (VRF) and Violation Severity Level (VSL) for each requirement in the CIP Cyber Security Standards revisions that address the Order No. 791 identify, assess, and correct; low impact; transient devices; and communication networks directives.

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

The CIP Version 5 Revisions Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria – VRFs

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC VRF Guidelines

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the VRF Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria - VSLs

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on the guidelines shown in the table below:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital Component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC Orders on VSLs

In its June 19, 2008 Order on VSLs, FERC indicated it would use the following four guidelines for determining whether to approve VSLs:

Guideline 1: VSL Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

- Compare the VSLs to any prior Levels of Non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when Levels of Non-compliance were used.

Guideline 2: VSL Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

- Guideline 2a: A violation of a "binary" type requirement must be a "Severe" VSL.
- Guideline 2b: Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: VSL Assignment Should Be Consistent with the Corresponding Requirement

- VSLs should not expand on what is required in the requirement.

Guideline 4: VSL Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

In its March 18, 2010 Order Addressing VSL Assignments in CIP Standards, FERC offered the following additional guidance relative to VSLs for CIP requirements:

Guideline 5: Requirements Where Single Lapse in Protection Result in Compromised Computer Network Security

Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary rather than gradated Violation Severity Levels.

Guideline 6: VSLs Should Account for Interdependent Tasks

Violation Severity Levels for cyber security Requirements containing interdependent tasks of documentation and implementation should account for their interdependence.

VRF and VSL Justifications – CIP-003-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Security policies enable effective implementation of the CIP standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. Periodic review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. Failure to provide clear governance may lead to ineffective controls, which could compromise security; and, therefore, the integrity of the Bulk Electric System. Consequently, a VRF of Medium was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security policy that contains certain elements specified in the requirement. The VRF is only applied at the requirement level, and the requirement parts are treated in aggregate. While the requirement specifies a number of elements, not necessarily parts, that must be included in the cyber security policy, the VRF is reflective of the policy as a whole. Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards.

VRF and VSL Justifications – CIP-003-6, R1			
	This requirement maps from CIP-003-5, R1, which has an approved VRF of Medium; therefore, the proposed VRF remains consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security policy is unlikely, under Emergency, abnormal, or restoration conditions anticipated by the preparations to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Therefore, this requirement was assigned a Medium VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security policy requirement encompasses a number of policy domains. The VRF is identified at the risk level represented by all of the policy domains in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact

VRF and VSL Justifications – CIP-003-6, R1			
or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR	or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR	policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but	and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing

VRF and VSL Justifications – CIP-003-6, R1			
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the	The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the	did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal	low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VRF and VSL Justifications – CIP-003-6, R1			
one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	to 18 calendar months of the previous approval. (R1.2)	

VRF and VSL Justifications – CIP-003-6, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to previously approved requirements CIP-003-5 R1 and CIP-003-5 R1.2. The VSLs were combined for these requirements using a gradated methodology. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-003-6, R1	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement; and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.

VRF and VSL Justifications – CIP-003-6, R1	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required topics. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-6, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of plans is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan,

VRF and VSL Justifications – CIP-003-6, R2	
	Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in the Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-5, R1, which has an approved VRF of Lower but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security plan would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VRF and VSL Justifications – CIP-003-6, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2)

VRF and VSL Justifications – CIP-003-6, R2			
Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2)	6, Requirement R2, Attachment 1, Section 4. (R2) (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems,	003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)	

VRF and VSL Justifications – CIP-003-6, R2			
	but failed to document physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)	OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2)	

VRF and VSL Justifications – CIP-003-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented its cyber security plan(s) but fails to address one or more of the required sections of the cyber security plan(s). The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-003-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept and incorporated the elements of the Attachment 1 but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-003-6, R2	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.

VRF and VSL Justifications – CIP-003-6, R2	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-6, R4	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability purpose of this requirement is to ensure clear lines of authority and ownership for security matters that could impact the stability and integrity of the Bulk Electric System, that delegations are kept up-to-date, and that individuals do not assume undocumented authority. As this requirement is only a part of the overall governance structure of a cyber security program, which includes additional leadership and policy, a VRF of Lower was assigned to this requirement.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement directs that the CIP Senior Manager is responsible for all approval and authorizations, but also grants the CIP Senior Manager with the ability to delegate this authority. The Requirement also calls for changes to the CIP Senior Manager and any delegations to be documented within 30 calendar days. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The requirement does not contain parts and are, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-003-5, R4, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to show clear authorization for actions taken back to the CIP Senior Manager would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The obligation of this requirement is to demonstrate that the CIP Senior Manager is ultimately responsible for all approvals and authorizations required in the CIP Standards. This requirement allows for delegation, but also obligates the Responsible Entity to document these delegations. The VRF was chosen based upon the highest reliability risk objective, which is the clear line of authority to the CIP Senior Manager and are, therefore, consistent with VRF Guideline 5.

VRF and VSL Justifications – CIP-003-6, R4			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

VRF and VSL Justifications – CIP-003-6, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. There is a single element upon which severity may be gradated; as such, gradated VSLs were assigned.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-003-5 R4. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-003-6, R4	
Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The requirement contains interdependent tasks of documentation and implementation. The VSL requirement presumes that the only way to demonstrate compliance is through documentation; as such, the VSLs are based upon the documentation measure, and implementation is assumed with documentation, therefore accounting for the interdependence in these tasks.

VRF and VSL Justifications – CIP-004-6, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective would not have adverse effect on the electrical state or capability of the Bulk Electric System.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-5.1, R2, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a training program would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity implemented a cyber security training program but failed to include one of	The Responsible Entity implemented a cyber security training program but failed to include two of the training	The Responsible Entity implemented a cyber security training program but failed to include three of the training	The Responsible Entity did not implement a cyber security training program appropriate to

VRF and VSL Justifications – CIP-004-6, R2			
the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals

VRF and VSL Justifications – CIP-004-6, R2			
			with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)

VRF and VSL Justifications – CIP-004-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-004-6, R2	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation,	The VSLs are based on a single violation and not cumulative violations.

VRF and VSL Justifications – CIP-004-6, R2	
Not on A Cumulative Number of Violations	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This VSL accounts for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation.

VRF and VSL Justifications – CIP-004-6, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.

VRF and VSL Justifications – CIP-004-6, R3	
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for implementing a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the Requirement level and the requirement parts are treated equally. Each Requirement Part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-5.1, R2, which has an approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a security training program could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining

VRF and VSL Justifications – CIP-004-6, R3			
physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR	physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical	authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR

VRF and VSL Justifications – CIP-004-6, R3			
The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or

VRF and VSL Justifications – CIP-004-6, R3			
			more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)

VRF and VSL Justifications – CIP-004-6, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R3. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations. The requirement is to implement a training program and failure for a single individual to have training does not necessarily imply a single violation. An overall view of the training program must consider the number of individuals who failed to receive training for a given period.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security. Although failure to implement a training program could associatively affect the ways in which computer network security applies, it does not, by itself, indicate a failure of computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This Requirement pertains to implementing the cyber security program and does not require procedural documentation.

VRF and VSL Justifications – CIP-004-6, R4			
Proposed VRF	**LOWER**		
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have received a personnel risk assessment. Failure to meet this objective could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for a personnel risk assessment program for individuals needing or having access to a BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement's VRF is consistent with similar security requirements with similar risks in the other CIP standards.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a personnel risk assessment program could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that documentation a personnel risk assessment is developed for individuals with access to BES Cyber Systems and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter	The Responsible Entity did not implement any documented program(s) for access management. (R4)

VRF and VSL Justifications – CIP-004-6, R4			
during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and	during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and	but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10%	OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

VRF and VSL Justifications – CIP-004-6, R4			
necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of itsBES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

VRF and VSL Justifications – CIP-004-6, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R4. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document or implement all required documented program(s) has a binary Severe VSL. Other Requirement Parts associated with the required processes do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-004-6, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Failure to revoke access to BES Cyber Systems and BES Cyber System Information within the required time frame is an administrative requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to revoke access to BES Cyber Systems and BES Cyber System Information when individuals no longer need access. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. Each Requirement row contributes to the objective of this Requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-5.1, R5, which has an approved VRF of Medium. Therefore, the proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to revoke access to BES Cyber Systems and BES Cyber System Information may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this Requirement, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Requirement R5 requires prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Each part of Requirement R5 specifies the obligations to revoke access in various situations when an individual no longer needs such access.

VRF and VSL Justifications – CIP-004-6, R5			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following

VRF and VSL Justifications – CIP-004-6, R5			
The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)	day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

VRF and VSL Justifications – CIP-004-6, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R5. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R5	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to implement programs for access revocation has a binary Severe VSL. A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-006-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this Requirement. The requirement specifies that each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. Failure to restrict physical access to BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets could result in unauthorized access, which could directly affect the ability to monitor or control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-5, R1, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-6, R1 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-006-6, Requirement R1 requires the implementation of documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. A failure to implement these documented plans may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this requirement,

VRF and VSL Justifications – CIP-006-6, R1			
	if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2)

VRF and VSL Justifications – CIP-006-6, R1			
			OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each

VRF and VSL Justifications – CIP-006-6, R1			
			Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR

VRF and VSL Justifications – CIP-006-6, R1			
			The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-006-5 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary in the "Severe" category and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

VRF and VSL Justifications – CIP-006-6, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. This Requirement calls for one or more documented visitor control programs. Failure to implement a visitor control program is not expected to directly affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented visitor control programs. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-5, R2, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-6, R2 is consistent.

VRF and VSL Justifications – CIP-006-6, R2			
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a documented visitor control program is an administrative requirement, and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented visitor control programs and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR

VRF and VSL Justifications – CIP-006-6, R2			
			The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are binary in the “Severe” category and therefore do not lower the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary in the “Severe” category and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

VRF and VSL Justifications – CIP-007-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The Requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports. Depending on the port and the impact classification of the affected cyber asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the Requirement level, and the Requirement Parts are treated equally. Unprotected logical and physical ports are both access points into a BES Cyber System.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R1, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs.

VRF and VSL Justifications – CIP-007-6, R1			
	Failure to disable or prevent access to a single logical or physical port on one BES Cyber System is unlikely to lead to Bulk Electric System instability, separation, or cascading failures. Therefore, this Requirement was assigned a Medium VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Unprotected logical and physical ports are both access points into a BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)

VRF and VSL Justifications – CIP-007-6, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-007-5 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement at the moderate or high VSL category would not necessarily compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R2			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The Requirement requires entities to manage security patches in a proactive way by monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner. Depending on the patch and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-007-5, R2, which has an approved VRF of Medium. Therefore the VRF is consistent with the FERC-approved VRF.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage a security patch on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R2. (R2) OR

VRF and VSL Justifications – CIP-007-6, R2			
evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan	OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

VRF and VSL Justifications – CIP-007-6, R2			
	within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)		

VRF and VSL Justifications – CIP-007-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines— There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but failed to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement a security patch can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability. There may be instances where the security vulnerability is so severe that failure to patch alone can comprise computer network security, but these cases are the exception.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R3			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The requirement requires entities to have processes to limit and detect the introduction of malicious code onto the components of a BES Cyber System. Depending on the malware and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R3, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage malicious code on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR

VRF and VSL Justifications – CIP-007-6, R3			
		The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

VRF and VSL Justifications – CIP-007-6, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R3. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement malicious code protections can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R4			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The requirement requires entities to have processes to provide security event monitoring with the purpose of detecting unauthorized access, reconnaissance, and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. Depending on the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R4, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage security events on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by	The Responsible Entity did not implement or document one or more process(es) that included the

VRF and VSL Justifications – CIP-007-6, R4			
Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (4.4)	applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

VRF and VSL Justifications – CIP-007-6, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R4. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the Requirement.

VRF and VSL Justifications – CIP-007-6, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement Parts for logging required types of events have a binary Severe VSL. Other Requirement Parts associated with security event monitoring do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities establish, implement, and document controls for electronic access to BES Cyber Systems. This includes enforcement of authentication for all user access and CIP Senior Manager, or delegate authorization for use of administrator, shared, default, and other generic account types. It prescribes procedural controls and conditions for changing default passwords and enforcing specific parameters for password based user authentication. Finally, it helps establish a process to limit (where technically feasible) unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for specific actions represented by multiple sub-requirements with a common set of objectives – to ensure the appropriate controls are in place for authorizing and establishing secure electronic access to BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007-5, R5, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement CIP Senior Manager oversight and establish controls to protect BES Cyber Systems from unauthorized electronic access could result in unauthorized access and could directly affect the ability to monitor or control the BES. Although the previous standards versions assigned a VRF of Severe, this is not consistent with the projected risk of BES Cyber System exploitation, which is why the VRF has been modified to Medium.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R5 have a common objective to provide controls to protect against unauthorized electronic access to BES Cyber Systems. The Requirements to authorize and review access, and the

VRF and VSL Justifications – CIP-007-6, R5			
	provided technical and procedural controls to prevent unauthorized access both specify the obligations to provide strong controls to monitor and control electronic access.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

VRF and VSL Justifications – CIP-007-6, R5			
		interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not

VRF and VSL Justifications – CIP-007-6, R5			
			technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

VRF and VSL Justifications – CIP-007-6, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R5. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R5	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations. Gradations are based on the number of unidentified account types, or number of missed controls for authentication and access represent components of the overall requirement that are necessary to fully achieve the reliability of the main requirement.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement parts that can compromise computer network security have a Severe VSL. Other Requirement Parts associated with system access control do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-009-6, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement's VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of implementing and maintaining the recovery plan.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-009-5, R2, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement and maintain the recovery plan is an administrative Requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common objective of implementing and maintaining recovery plans. Requirement Rows 2.1 and 2.3 specify the obligation to implement and test the plan. Requirement Row 2.2 specifies the obligation to maintain backup information used to recover the BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1)

VRF and VSL Justifications – CIP-009-6, R2			
between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

VRF and VSL Justifications – CIP-009-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-009-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-009-6, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this requirement indicates the recovery plan was not properly tested and may have deficiencies, but a violation cannot immediately compromise computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This Requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-010-2, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration change management processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration change management processes can have a medium impact on the reliability and operability of the BES. Although the requirement is administrative in nature and is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration change management. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, R1 specifies the implementation of documented configuration change management processes in conjunction with CIP-010-2, R2, which specifies the implementation of documented configuration monitoring processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R1 requires the implementation of documented configuration change management processes. A failure to implement these documented processes has medium impact on the

VRF and VSL Justifications – CIP-010-2, R1			
	reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-2, Requirement R1 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that

VRF and VSL Justifications – CIP-010-2, R1			
			deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did

VRF and VSL Justifications – CIP-010-2, R1			
			not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

VRF and VSL Justifications – CIP-010-2, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-010-1 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection is not expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R1 specifies that a Responsible Entity must implement and document the processes for configuration change management of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration change management process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-2, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration monitoring processes. A VRF assignment of Medium is consistent with the lower risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration monitoring processes has medium impact on the reliability and operability of the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration monitoring. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, R2 specifies the implementation of documented configuration monitoring processes in conjunction with CIP-010-2, R1, which specifies the implementation of documented configuration change management processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R2 requires the implementation of documented configuration monitoring processes. A failure to implement these documented processes has medium impact on the reliability and operability of the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-010-2, R2			
	CIP-010-2, Requirement R2 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)

VRF and VSL Justifications – CIP-010-2, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines — Severe: the performance measured does not substantively meet the intent of the Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-010-1 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The VSL is binary.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R2 specifies that a Responsible Entity must implement and document the processes for configuration monitoring of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration monitoring process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-2, R4	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement plan(s) that are intended to prevent

VRF and VSL Justifications – CIP-010-2, R4	
	Transient Cyber Assets and Removable Media from introducing malicious code to BES Cyber Systems. The impact of a failure to implement documented plans can have a medium impact on the reliability and operability of the BES. If violated, the requirement poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented plans that are intended to prevent Transient Cyber Assets and Removable Media from introducing malicious code to BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, Requirement R4 incorporates the concepts from other CIP requirements to define requirements for Transient Cyber Assets and Removable Media. Similar to other requirements, CIP-010-2, Requirement R4 has a medium risk impact of a violation to implement documented plan(s) and, therefore, has a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R4 requires the implementation of documented plans for Transient Cyber Assets and Removable Media. A failure to implement these documented plans has medium impact on the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-010-2, R4			
	CIP-010-2, Requirement R4 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-2, Requirement R4. (R4)

VRF and VSL Justifications – CIP-010-2, R4			
Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)	OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

VRF and VSL Justifications – CIP-010-2, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security plans but fails to address one or more of the required sections of the cyber security plans. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	CIP-010-2, Requirement R4 is a new requirement and raises the level of compliance from the previous version where certain Protected Cyber Assets did not have any requirements applied.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection is not expected to compromise computer network security. Failure to implement the Transient Cyber Asset and Removable Media plan can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail to actuate the vulnerability. There may be instances where the security vulnerability is so severe that failure to implement transient device protections can comprise computer network security, but these cases are the exception.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R4 specifies that a Responsible Entity must implement and document the plan(s) for Transient Cyber Assets and Removable Media. Documentation of these plan(s) is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan(s) in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required sections of the cyber security plan(s). The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-011-2, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities prevent unauthorized access to BES Cyber System Information. Failure to adequately identify, protect, and control access to such information could result in unauthorized access and lost, stolen, or misused Cyber System Information. Such failure represents a risk to the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for methods to identify, provide secure handling, and control access to Cyber System Information. The VRF is only applied at the requirement level and the requirement parts are treated equally. The identification, secure handling and control of access have the common objective to protect BES Cyber System Information.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-003, R4 and CIP-003-3, R4.1, which have an approved VRF of Medium. The Requirement also maps to CIP-003-3, R4.2 and CIP-003-3, R4.3 and to CIP-003-3, R5, CIP-003-3, R5.1, CIP-003-3, R5.2, and CIP-003-3, R5.3, which have an approved VRF of Lower. The requirement has the object of securing Cyber System Information. Version 5 combines requirements to ensure consistency. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately identify and protect BES Cyber System Information could result in disclosure of information to unauthorized persons, lost, stolen, or misused Cyber System Information. Such breaches of confidentiality represent a risk to the reliability of Bulk Electric System from misuse by unauthorized persons.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-011-2, R1			
	The sub requirements in R1 have a common objective to assure confidentiality of BES Cyber System Information. The obligations to identify, control access, and assure proper handling of BES Cyber System Information contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

VRF and VSL Justifications – CIP-011-2, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-011-1 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-011-2, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The VSLs are binary for this requirement.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

Exhibit F

Summary of Development History and Record of Development

Summary of Development

Summary of Development History

The development record for proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 is summarized below.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived, in part, from the standard drafting team. For this project, the standard drafting team consisted of industry experts, all with a diverse set of experiences. A roster of the standard drafting team members is included in Exhibit G.

II. Standard Development History

A. Standard Authorization Request Development

A Standard Authorization Request ("SAR") was submitted on January 7, 2014 to the Standards Committee ("SC") and accepted by the SC on January 15, 2014 for a thirty-day informal comment period. After reviewing the comments, NERC posted a revised SAR on March 17, 2014.

B. First Posting-Comment Period and Ballot

Proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 were posted for a 45-day public comment period from June 2, 2014 through July 16, 2014, with an initial ballot held from July 7, 2014 through July 16, 2014. Several documents were posted for guidance with the first drafts, including the proposed Reliability Standards, new and modified definition of terms used in the standards for incorporation into the NERC Glossary, the associated Implementation Plan, Consideration of

[1] Section 215(d) (2) of the Federal Power Act; 16 U.S.C. §824(d) (2) (2006).

Issues and Directives, Mapping Document, and *"Identify, Assess, and Correct" and Reliability Assurance Initiative FAQs*. Each of the posted Reliability Standards included revisions to address the "identify, assess, and correct" directive. Proposed Reliability Standards CIP-006-6 and CIP-007-6 also included revisions to address the communication networks directive, and proposed Reliability Standard CIP-003-6 included revisions to address the low impact directive. The transient device directive was addressed primarily in proposed Reliability Standard CIP-010-2, but the standard drafting team also made minor revisions in CIP-004-6, CIP-007-6, and CIP-011-2 to address this directive.

The results of the initial ballots were as follows:

- CIP-003-6 received a 80.73% quorum and an approval of 35.67%;
- CIP-004-6 received a 80.49% quorum and an approval of 80.76%;
- CIP-006-6 received a 80.00% quorum and an approval of 76.24%;
- CIP-007-6 received a 80.24% quorum and an approval of 78.41%;
- CIP-009-6 received a 80.24% quorum and an approval of 85.32%;
- CIP-010-2 received a 80.49% quorum and an approval of 49.42%; and
- CIP-011-2 received a 80.24% quorum and an approval of 82.55%.[2]

There were 98 sets of comments on the initial posting, including comments from approximately 196 different individuals from approximately 142 companies representing all 10 of the industry segments. The comments are available at:

---

[2] The results of the Non-Binding Polls for the VRFs and VSLs were as follows: Reliability Standards CIP-003-6 achieved a 77.81% quorum and a 31.86% of supportive opinions; CIP-004-6 achieved a 77.27% quorum and a 77.63% of supportive opinions; CIP-006-6 achieved a 77.27% quorum and a 74.56% of supportive opinions; CIP-007-6 achieved a 77.27% quorum and a 75.44% of supportive opinions; CIP-009-6 achieved a 77.27% quorum and a 85.59% of supportive opinions; CIP-010-2 achieved a 77.54% quorum and a 39.04% of supportive opinions; and CIP-011-2 achieved a 77.01% quorum and a 79.74% of supportive opinions.

http://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/Comments%20Received-%202014-02%20CIP%20V5%20June%202014.pdf.

C. Second Posting - Additional 45-Day Comment Period Ballot

Based on the results of the initial ballot and the comments received, NERC posted revised drafts of proposed Reliability Standards CIP-003-6 and CIP-010-2, the new and modified definitions used in those standards, and the associated Implementation Plan for a 45-day public comment period from September 3, 2014 through October 17, 2014, with an additional ballot held from October 8, 2014 through October 17, 2014. The second posting of these standards reflected changes the standard drafting team made after considering all comments on the initial drafts of the standards. For a description of the changes, please see the Consideration of Comments on Draft 1, available at: http://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/Consideration_of_Comments_to_Initial_Posting_of_CIP_V5_Revisions_09032014.pdf.

Additionally, to ensure that NERC could satisfy its regulatory deadline, NERC posted for a 45-day comment period and ballot versions of Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 that only addressed the "identify, assess, and correct" and communication network directives. To avoid confusion, these versions were posted as CIP-003-X, CIP-004-X, CIP-007-X, CIP-010-X, and CIP-011-X.

The results of the additional ballots were as follows:

- Each of the –X versions received a 84.63% quorum and an approval of 93.21%;
- CIP-003-6 received a 84.15% quorum and an approval of 68.09%; and
- CIP-010-2 received a 84.15% quorum and an approval of 74.25%.[3]

[3] The proposed definitions and associated implementation plans also received the requisite approval.

There were 70 sets of comments on the additional ballots, including comments from approximately 164 different individuals from approximately 117 companies representing 9 of the 10 of the industry segments. The comments are available at: http://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/Comments_Received_2014-02_CIP_V5_10292014.pdf.

D. Third Posting – Additional 45-Day Comment Period and Ballot

Although each of the proposed Reliability Standards received the requisite approval in the second posting, after reviewing industry comment, the standard drafting team determined that additional modifications to Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 were necessary to address industry comments on the modifications related to the low impact and transient device directives. On November 25, 2014, after the standard drafting team addressed industry comment, NERC posted revised versions of proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 for an additional 45-day comment period and ballot.[4] For a description of the changes, please see the Consideration of Comments on Draft 2, available at: http://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/Consideration_of_Comments_to_Additional_Posting_of_CIP_V5_Revisions_Third_Posting.pdf.

The results of the additional ballots were as follows:

- CIP-003-6 received a 81.22% quorum and an approval of 81.92%;
- CIP-004-6 received a 81.71% quorum and an approval of 98.89%;

[4] During development, these revised versions of the proposed Reliability Standards were posted as CIP-003-7, CIP-004-7, CIP-007-7, CIP-10-3, and CIP-011-3 to help differentiate the revised versions from the versions adopted by the Board in November 2014. For purposes of Board adoption and filing with applicable governmental authorities, however, the version numbers are presented as -6 and -2 because the versions adopted by the Board in November 2014 were never filed with applicable governmental authorities.

- CIP-007-6 received a 81.46% quorum and an approval of 98.86%;
- CIP-010-2 received a 81.71% quorum and an approval of 88.13%; and
- CIP-0011-2 received a 81.71% quorum and an approval of 98.89%.[5]

There were 66 sets of comments on the additional ballots, including comments from approximately 143 different individuals from approximately 99 companies representing all 10 industry segments. The comments are available at: http://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/Comments%20Received%202014-02%20CIP%20V5%20November%202014.pdf. After reviewing the comments, the SDT determined that no further substantive revisions were necessary, as discussed in the Consideration of Comments on the third posting, available at: http://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/Consideration_of_Comments_to_Additional_Posting_of_CIP_V5_Revisions_January_23_FB.pdf.

E. Final Ballots

To ensure that it could meet its regulatory deadline, on October 28, 2014, NERC posted for final ballot the versions of the proposed Reliability Standards that only addressed the "identify, assess, and correct" and communication network directives. Proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, CIP-011-2 were posted for a 10-day final ballot period from October 28, 2014 through November 6, 2014. The results of those final ballots were as follows:

- CIP-003-6 achieved quorum of 87.56% and an approval of 83.84%;
- CIP-004-6 achieved quorum of 87.32% and an approval of 95.34%;
- CIP-006-6 achieved quorum of 87.07% and an approval of 86.00%.

[5] The proposed definitions and associated implementation plans also received the requisite approval.

- CIP-007-6 achieved quorum of 87.56% and an approval of 95.35%;
- CIP-009-6 achieved quorum of 87.56% and an approval of 91.17%;
- CIP-010-2 achieved quorum 87.80% and an approval of 83.88%; and
- CIP-011-2 achieved quorum of 87.56% and an approval of 95.40%.[6]

After the revised versions of Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 that also addressed the transient device and low impact directives received the requisite approval on the third posting, these standards were posted for a 10-day final ballot period from January 23, 2015 through February 2, 2015. The results of those final ballots were as follows:

- CIP-003-6 achieved quorum of 84.15% and an approval of 79.76%;
- CIP-004-6 achieved quorum of 84.39% and an approval of 98.94%;
- CIP-007-6 achieved quorum of 84.15% and an approval of 98.94%.
- CIP-010-2 achieved quorum 84.39% and an approval of 86.76%; and
- CIP-011-2 achieved quorum of 84.39% and an approval of 98.93%.[7]

F. Board of Trustees Approval

Proposed Reliability Standards CIP-006-6 and CIP-009-6 were approved by the NERC Board of Trustees on November 13, 2014. The revised drafts of CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 were approved by the NERC Board of Trustees on February 12, 2015.

---

6 The associated implementation plans also received the requisite approval.

7 The proposed definitions and associated implementation plans also received the requisite approval.

Complete Record of Development

Program Areas & Departments > Standards > Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions
Related Files

Status:

Final ballots for five **Critical Infrastructure Protection Standards Version 5 Revisions** standards, two definitions (within CIP-003 and standards addressing transient devices) and the implementation plan concluded at **8 p.m. Eastern Monday, February 2, 2015.** Voting results can be accessed via the links below. The standards will be submitted to the Board of Trustees (the Board) for adoption and then filed with the appropriate regulatory authorities.

The final ballots for the above-referenced Reliability Standards use the same version numbers from the prior additional ballot (i.e., -7 and -3). However, because these Reliability Standards are replacing the -6 and -2 versions of these Reliability Standards adopted by the Board in November 2014, which have not been filed with appropriate regulatory authorities, the version numbers will revert back to -6 and -2 when presented to the Board for adoption. The -7 and -3 version numbering was simply used during development to help differentiate the revised versions from the versions adopted by the Board in November.

Background:

On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards and also directed that NERC make the following modifications to those standards:

1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for Low Impact assets.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the "identify, assess, and correct" language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the Low Impact and transient electronic devices directives. The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft **CIP-003-7** — Cyber Security — Security Management Controls Clean | Redline to Last Posted Board Documents Clean CIP-003-6| Redline to Last Adopted **CIP-004-7** — Cyber Security — Personnel & Training Clean | Redline to Last Posted	Final Ballot Info>> Vote>> (Closed)	1/23/15 - 02/02/15	Summary>> Ballot Results CIP-003-7>> CIP-004-7>> CIP-007-7>> CIP-010-3>>	

Board Documents Clean CIP-004-6| Redline to Last Adopted **CIP-007-7** — Cyber Security — Systems Security Management Clean | Redline to Last Posted Board Documents Clean CIP-007-6| Redline to Last Adopted **CIP-010-3** — Cyber Security — Configuration Change Management & Vulnerability Assessments Clean | Redline to Last Posted Board Documents Clean CIP-010-2| Redline to Last Adopted **CIP-011-3** — Cyber Security — Information Protection Clean | Redline to Last Posted Board Documents Clean CIP-011-2| Redline to Last Adopted **Definition of Terms Used in CIP-003-7** Clean | Redline to Last Posted Board Documents Newly-Defined Definition of Terms Used in CIP-003-6 **Definition of Terms Regarding Transient Devices** Clean | Redline to Last Posted Board Documents Newly-Defined Terms Regarding Transient Devices | Modified Terms **Implementation Plan** Clean | Redline to Last Posted Board Documents Clean | Redline to Last Adopted			CIP-011-3>> CIP-003-7 Definition>> CIP-010-3 Definition>> Implementation Plan>>	

Supporting Documents: **Consideration of Issues and Directives** Clean | Redline to Last Posted **Mapping Document** Clean | Redline to Last Posted **VRF/VSL Justification** Clean | Board				
Draft 3 **CIP-003-7** — Cyber Security — Security Management Controls Clean | Redline to Last Posted **CIP-004-7** — Cyber Security — Personnel & Training Clean | Redline to Last Posted **CIP-007-7** — Cyber Security — Systems Security Management Clean | Redline to Last Posted **CIP-010-3** — Cyber Security — Configuration Change Management & Vulnerability Assessments Clean | Redline to Last Posted **CIP-011-3** — Cyber Security — Information Protection Clean | Redline to Last Posted **Definition of Terms Used in CIP-003-7** Clean | Redline to Last Posted **Definition of Terms Regarding Transient Devices** Clean | Redline to Last Posted **Implementation Plan** Clean | Redline to Last Posted **Supporting Documents:** Unofficial Comment Form (Word)	Additional Ballots and Non-Binding Polls Updated Info>> Info>> Vote>> (Closed)	12/30/14 -01/09/15	Summary>> Ballot Results CIP-003-7>> CIP-004-7>> CIP-007-7>> CIP-010-3>> CIP-011-3>> CIP-003-7 Definition>> CIP-010-3 Definition>> Implementation Plan>> Non-Binding Poll Results CIP-003-7>> CIP-004-7>> CIP-007-7>> CIP-010-3>> CIP-011-3>>	Consideration of Comments>>

<table>
<tr><td rowspan="2">Consideration of Issues and Directives
Clean | Redline to Last Posted

Mapping Document
Clean | Redline to Last Posted

Draft RSAWs
CIP-002-5.1

CIP-003-7

CIP-004-7

CIP-005-5

CIP-006-6

CIP-007-7

CIP-008-5

CIP-009-6

CIP-010-3

CIP-011-3</td><td>Comment Period

Info>>

Submit Comments>>

(Closed)</td><td>11/25/14 –01/09/15</td><td rowspan="2">Comments Received>></td><td rowspan="2"></td></tr>
<tr><td colspan="2">The comment period and additional ballot close dates were extended one day to January 9, 2015 due to a NERC.com maintenance outage that occurred Saturday, December 13, 2014.</td></tr>
<tr><td>Please send RSAW Feedback to:

RSAWfeedback@nerc.net</td><td>12/10/14 - 01/09/15</td><td colspan="3"></td></tr>
</table>

Final Draft **CIP-003-6** — Cyber Security — Security Management Controls Clean **(95)** | Redline to Last Posted **(96)** Redline to CIP-003-5 **(97)** **CIP-004-6** — Cyber Security — Personnel & Training Clean **(98)** | Redline to Last Posted **(99)** Redline to CIP-004-5.1 **(100)** **CIP-006-6** — Cyber Security — Physical Security of BES Cyber Systems Clean **(101)** | Redline to Last Posted **(102)** Redline to CIP-006-5 **(103)** **CIP-007-6** — Cyber Security — Systems Security Management Clean **(104)** | Redline to Last Posted **(105)** Redline to CIP-007-5 **(106)** **CIP-009-6** — Cyber Security — Recovery Plans for BES Cyber Systems Clean **(107)** | Redline to Last Posted **(108)** Redline to CIP-009-5 **(109)** **CIP-010-2** — Cyber Security — Configuration ChangeManagement and Vulnerability Assessments Clean **(110)** | Redline to Last Posted **(111)** Redline to CIP-010-1 **(112)** **CIP-011-2** — Cyber Security — Information Protection Clean **(113)** | Redline **(114)** Redline to CIP-011-1 **(115)**	Final Ballots Info>> **(123)** Vote>> (Closed)	10/28/14 - 11/06/14	Summary>> **(124)** Ballot Results CIP-003-6>> **(125)** CIP-004-6>> **(126)** CIP-006-6>> **(127)** CIP-007-6>> **(128)** CIP-009-6>> **(129)** CIP-010-2>> **(130)** CIP-011-2>> **(131)** Implementation Plan>> **(132)**	

Implementation Plan Clean **(116)** | Redline to Last Posted **(117)** **Consideration of Issues and Directives** Clean **(118)** | Redline to Last Posted **(119)** **Mapping Document** Clean **(120)** | Redline to Last Posted **(121)** **Supporting Documents:** VRF/VSL Justification **(122)**				
Draft 2 **CIP-003-6** — Cyber Security — Security Management Controls Clean **(49)** | Redline to Last Posted **(50)** **CIP-010-2** — Cyber Security — Configuration Change Management Clean **(51)** | Redline to Last Posted **(52)** **CIP-003-X** — Cyber Security — Security Management Controls Clean **(53)** | Redline **(54)** **CIP-004-X** — Cyber Security — Personnel and Training Clean **(55)** | Redline **(56)** **CIP-007-X** — Cyber Security — Systems Security Management Clean **(57)** | Redline **(58)** **CIP-010-X** — Cyber Security — Configuration Change Management Clean **(59)** | Redline **(60)**	Additional Ballots and Non-Binding Polls Updated Info>> **(75)** Info>> **(76)** Vote>> (Closed)	10/08/14 - 10/17/14	Summary>> **(78)** Ballot Results CIP Version X>> **(79)** CIP-003-6>> **(80)** CIP-010-2>> **(81)** Definition CIP-003-6>> **(82)** Definition CIP-010-2>> **(83)** Implementation Plan>> **(84)** Non-Binding Poll Results CIP-003-X>> **(85)** CIP-003-6>> **(86)**	

<table>
<tr>
<td rowspan="3">CIP-011-X — Cyber Security — Information Protection
Clean (61) | Redline (62)

Definition of Terms Used in CIP-003-6 (63)

Definition of Terms Used in CIP-010-2
Clean (64) | Redline to Last Posted (65)

Implementation Plan
Clean (66) | Redline to Last Posted (67)

Implementation Plan (-X Posting) (68)

Supporting Documents
Unofficial Comment Form (Word) (69)

IAC Posting - X Explanation (70)

Consideration of Issues and Directives
Clean (71) | Redline to Last Posted (72)

Mapping Document
Clean (73) | Redline to Last Posted (74)

Draft RSAWs

CIP-002-5.1

CIP-003-6

CIP-004-6

CIP-005-5

CIP-006-6

CIP-007-6

CIP-008-5

CIP-009-6

CIP-010-2

CIP-011-2</td>
<td></td>
<td></td>
<td>CIP-004-X>>
(87)

CIP-007-X>>
(88)

CIP-010-X>>
(89)

CIP-010-2>>
(90)

CIP-011-X>>
(91)</td>
<td></td>
</tr>
<tr>
<td>Comment Period

Info>> (77)

Submit Comments>>

(Closed)</td>
<td>09/03/14 - 10/17/14</td>
<td>Comments Received>>
(92)</td>
<td>Updated Consideration of Comments>>
(93)

Consideration of Comments>>
(94)</td>
</tr>
<tr>
<td>Please send RSAW Feedback to:

RSAWfeedback@nerc.net

(Closed)</td>
<td>09/17/14 - 10/17/14</td>
<td></td>
<td></td>
</tr>
</table>

CIP-003-6 — Cyber Security — Security Management Controls Clean **(7)** | Redline **(8)** **CIP-004-6** — Cyber Security — Personnel and Training Clean **(9)** | Redline **(10)** **CIP-006-6** — Cyber Security — Physical Security Clean **(11)** | Redline **(12)** **CIP-007-6** — Cyber Security — Systems Security Management Clean **(13)** | Redline **(14)** **CIP-009-6** — Cyber Security — Recovery Plans for BES Cyber Systems Clean **(15)** | Redline **(16)** **CIP-010-2** — Cyber Security — Configuration Change Management Clean **(17)** | Redline **(18)** **CIP-011-2** — Cyber Security — Information Protection Clean **(19)** | Redline **(20)** **Definition of Terms Used in Standards** Clean **(21)** | Redline **(22)** Implementation Plan **(23)** **Supporting Documents** Unofficial Comment Form (Word) **(24)** Consideration of Issues and Directives **(25)** Mapping Document **(26)** "Identify, Assess, and Correct" and Reliability Assurance Initiative FAQs **(27)**	Ballots and Non-Binding Polls Updated Info>> **(28)** Info>> **(29)** Vote>> (Closed)	07/07/14 - 07/16/14	Summary>> **(31)** Ballot Results CIP-003-6>> **(32)** CIP-004-6>> **(33)** CIP-006-6>> **(34)** CIP-007-6>> **(35)** CIP-009-6>> **(36)** CIP-010-2>> **(37)** CIP-011-2>> **(38)** Definition>> **(39)** Non-Binding Poll Results CIP-003-6>> **(40)** CIP-004-6>> **(41)** CIP-006-6>> **(42)** CIP-007-6>> **(43)**	

Draft RSAWs CIP-002-5.1 CIP-003-6 CIP-004-6 CIP-005-5 CIP-006-6 CIP-007-6 CIP-008-5 CIP-009-6 CIP-010-2 CIP-011-2			CIP-009-6>> **(44)** CIP-010-2>> **(45)** CIP-011-2>> **(46)**	
	Comment Period Info>> **(30)** Submit Comments>> (Closed)	06/02/14 - 07/16/14	Comments Received>> **(47)**	Consideration of Comments>> **(48)**
	Join Ballot Pool>> Please note: To avoid the inconvenience for the industry to join 15 separate ballot pools, we have set up one for the ballots (on the standards and definition) and one for the non-binding polls. Once the ballot pools close, individual ballots will be created by carrying over the members of the ballot pools. There will be a separate ballot for each of the 7 standards, the definition and 7 non-binding polls. (Closed)	06/02/14 - 07/01/14		
	Please send RSAW Feedback to: RSAWfeedback@nerc.net (Closed)	06/17/14 - 07/16/14		
SAR Clean **(5)** | Redline to last posted **(6)**				
Standard Authorization Request **(1)**	Comment Period Info>> **(3)** Submit Comments>> (Closed)	01/17/14 - 02/18/14	Comments Received>> **(4)**	

Supporting Documents: Unofficial Comment Form (Word) **(2)**				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, please email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the Bulk-Power System through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Cyber Security Standards		
Date Submitted:	January 15, 2014		
SAR Requester Information			
Name:	Ryan Stewart		
Organization:	NERC		
Telephone:	404-446-2569	E-mail:	Ryan.Stewart@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.
Industry Need (What is the industry problem this request is trying to solve?):
On November 22, 2013, FERC issued Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*. In this order, FERC approved version 5 of the CIP standards, and also directed that NERC make the following modifications to those standards:

SAR Information
1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements. 2. Develop modifications to the CIP standards to address security controls for Low Impact assets. 3. Develop requirements that protect transient electronic devices. 4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks. FERC directed NERC to submit new or modified standards responding to the directives related to the "identify, assess, and correct" language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the Low Impact and transient electronic devices directives.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The proposed project will develop new or modify existing requirements in the CIP standards to address the directives from FERC Order No. 791. This project may also consider input that may be provided from CIP version 5 transition activities, for example from the NERC transition study or CIP Version 5 transition program.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
As stated above, the purpose of the proposed project is to respond to the directives in FERC Order No. 791 and to respond within the timeframe required by the order for the directives related to the "identify, assess, and correct" language and communication networks. The following is a description of the responses the standard drafting team (SDT) shall consider during development of the new or modified standards: • The SDT shall work to remove or modify the identify, access, and correct language. The SDT shall work with NERC compliance and enforcement staff to inform and educate stakeholders on the development of alternative approaches for accomplishing the goals underlying the inclusion of the identify, assess, and correct language without placing compliance language in those requirements. • The SDT shall consider the necessary standard modifications to be developed that address security controls for Low Impact assets. • The SDT shall consider whether any further standard protections are needed to address potential vulnerabilities associated with transient devices (*e.g.,* thumb drives and laptop

SAR Information
computers). During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards. • The SDT shall consider how to define the term "communications networks" and new or modified standard(s) that address the Commission's concerns for the protection of communication networks. As stated in Order No. 791, FERC staff will lead a technical conference that, among other things, will address the issue of protecting the non-programmable components of communication networks. The SDT shall review the technical conference testimony and comments to inform the development of the definition for communication networks and new or modified standards for the protection of communication networks. When developing these new or modified CIP standards, the SDT may consider input from CIP version 5 transition activities, such as from the NERC transition study or CIP Version 5 transition program.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.

Reliability Functions		
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected Bulk-Power Systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected Bulk-Power Systems shall be made available to those entities responsible for planning and operating the systems reliably.

Reliability and Market Interface Principles	
☐	4. Plans for emergency operation and system restoration of interconnected Bulk-Power Systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected Bulk-Power Systems.
☒	6. Personnel responsible for planning and operating interconnected Bulk-Power Systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected Bulk-Power Systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation
CIP-002-5.1	BES Cyber System Categorization
CIP-003-5	Security Management Controls
CIP-004-5.1	Personnel & Training
CIP-005-5	Electronic Security Perimeter(s)
CIP-006-5	Physical Security of BES Cyber Systems
CIP-007-5	Systems Security Management
CIP-008-5	Incident Reporting and Response Planning

Related Standards	
CIP-009-5	Recovery Plans for BES Cyber Systems
CIP-010-1	Configure Change Management and Vulnerability Assessments
CIP-011-1	Information Protection

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
ERCOT	None
FRCC	None
MRO	None
NPCC	None
RFC	None
SERC	None
SPP	None

Regional Variances	
WECC	None

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Standard Authorization Request – Cyber Security Standards

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the Standard Authorization Request (SAR). The electronic comment form must be completed by **8 p.m. Eastern, Tuesday, February 18, 2014**.

All documents and information about this project are available on the project page. If you have questions please contact Marisa Hecht at marisa.hecht@nerc.net or by telephone at 404-446-9620 or Ryan Stewart at ryan.stewart@nerc.net or by telephone at 404-446-2569.

Background Information

On November 22, 2013, FERC issued Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*. In this order, FERC approved version 5 of the CIP standards, and also directed that NERC make the following modifications to those standards:

1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for Low Impact assets.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the "identify, assess, and correct" language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the Low Impact and transient electronic devices directives.

On January 15, 2014, the NERC Standards Committee accepted the Standards Authorization Request (SAR) and authorized the posting of the CIP Version 5 Revisions SAR. It will be posted for a 30-day informal comment period because it is addressing FERC directives.

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No:

   Comments:

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

   Yes:

   No:

   Comments:

3. Are there any other concerns with this SAR that haven't been covered in previous questions?

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Informal Comment Period Now Open through February 18, 2014

Now Available

A 30-day informal comment period for the Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions Standard Authorization Request (SAR) is now open through **8 p.m. Eastern on Tuesday, February 18, 2014.**

Background information for this project can be found on the project page.

Instructions for Commenting

An informal comment period is open through **8 p.m. Eastern on Tuesday, February 18, 2014.** Please use the electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Individual or group. (34 Responses)
Name (23 Responses)
Organization (23 Responses)
Group Name (11 Responses)
Lead Contact (11 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (1 Responses)
Comments (34 Responses)
Question 1 (33 Responses)
Question 1 Comments (33 Responses)
Question 2 (33 Responses)
Question 2 Comments (33 Responses)
Question 3 (33 Responses)
Question 3 Comments (33 Responses)

Group
Dominion
Connie Lowe
Yes
No
No
Group
Colorado Springs Utilities
Shannon Fair
Yes
No
Yes
Identify, Assess, and Correct Compliance Language - We think the ‘identify, assess, and correct’ language is adequate if NERC defines what the minimum criteria is for each program being implemented. Requirements for Low Impact BES Cyber Systems - We think there should be guidance that establishes a baseline of minimum expectations for the four topic

areas, along with a definition of the minimum auditable documentation required to demonstrate compliance. 30-Day Exemption or exemption of transient devices from compliance with the standards - A 30 day exception could allow insecure devices to be introduced to the ESP. The definition of BES Cyber Asset should be extended to cover these types of devices. For example, transient systems could be defined as a specific type of Cyber Asset (perhaps as a Maintenance Cyber Asset or a Transient Cyber Asset) along with guidance on minimal security expectations for the new type of Cyber Asset. Survey of BES Cyber Assets that do not satisfy the"15-minute" parameter described in the Guidelines of CIP-002-5 - Any standard needs to clearly define how the 15-minute parameter should be applied. For example, is the 15 minutes applicable to normal operations, intentional misuse, or device failure?
Group
SRC
Greg Campoli
SRC, supported by CAISO, ERCOT, IESO, MISO, & PJM
Yes
No
Yes
CIP Version 5 is an important step forward for the electric subsector to continue to demonstrate leadership in the development of policy and regulations for securing critical infrastructure. The FERC Order 791 gives NERC a year to respond to significant items the commission identified. The SRC believes that establishing a Standard Drafting Team (SDT) to respond to the commission order is appropriate and necessary. It is important to note that adequate time should be provided to enable the SDT to assess and adopt the effective solutions to meet the items the commission is seeking. Depending on NERC's response to Order 791, the implementation timeline could be impacted, especially if the changes or guidance included in the response have significant impact on the implementation efforts. The RAI project is a multi-year initiative that NERC is currently pilot- testing to improve the compliance monitoring and audit process. The IRC believes RAI is a positive and promising approach but it needs to be vetted through the pilots and will not be ready for general-availability until 2015. NERC's proposal to use ES-C2M2 framework as a benchmark for CIP standards will require further evaluation and analysis before this can be understood and applied as a potential measurement solution linked to the NERC CIP standards. Before adopting ES-C2M2, NERC and the industry need to monitor and understand how CIP, RAI and ES-C2M2 would be integrated. If not addressed appropriately, incorporating the ES-C2M2 framework could drive significant scope expansion impacting both audits and ISO operational requirements. RAI is a voluntary program and the prototypes are scheduled for two more years making it difficult to link to the FERC one year requirement. Additionally RAI has not been tested in CIP at this time. ES-C2M2 is an enterprise risk program and audit

scope and standards links with CIP are unclear. There are concerns how RAI and ES-C2M2 fit into NERC scope as a solution. The SRC believes NERC should focus on RAI for now and incorporate ES-C2M2 at a later time. As it is, the RAI timeline is two years out. If ES-C2M2 is also bundled in, the industry will have to wait even longer. Incremental improvements are far easier and provide the flexibility to adapt to emerging risks and threats, rather than complete make-over's. The SRC agrees that the 'Indentify, Assess and Correct' (IAC) approach can be removed from the CIP Standards, while still avoiding a 'zero defect/tolerance' approach to standards enforcement. The Standards Drafting Team should work on developing a clear alternative that is acceptable to the industry, the regional entities, NERC and to FERC. SAR, Page3:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices. Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR. The Standard Drafting Team should consider a tiered approach when defining communication networks and standards to protect those elements. It doesn't have to be a one-size-fits-all. This is especially important for Physical protections. The SRC is committed to helping NERC respond to the commission's issues and will continue to provide support to the CIP Version 5 drafting team and RAI project initiatives.

Group

Northeast Power Corodinating Council

Guy Zito

No

: Recommend modifications to the SAR language to clarify and align with FERC order 791:SAR, page 3:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."• Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices.• Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR. NPCC recommends the following be considered: i) Suggest changing the

Detailed Description's second bullet to The SDT shall consider the development of necessary Standard modification or new Standards that address security controls for Low Impact assets. ii) Suggest splitting the Detailed Description's third bullet into two bullets for clarity. Replace this third bullet with the following a - c. a) The SDT shall consider how to define the term transient device. b) The SDT shall consider whether further Standard protections are needed to address vulnerabilities associated with transient devices. c) The SDT will review the results of the ERO survey concerning the use of the "15 minute" parameter to inform the SDT's development of a new / modified Standards for the protection of Cyber Assets and BES Cyber Systems from the vulnerability introduced by transient devices.
No
Yes
NERC staff requested that the industry not submit Requests for Interpretation (RFI). However, more detailed reviews of the approved CIP Version 5 Standards generated additional questions regarding com,pliance. NPCC members are requesting a process for seeking clarifications so that company implementation expectations of CIP Version 5 will be consistent with future audit expectations. Recommend removing the “identify, assess, and correct” language in 17 CIP Version 5 requirements. Recommend that the Standard Drafting Team develop a new standard that will allow allow this one standard to have an implementation date later than the other Version 5 standards. Low Impact assets, like substations, are often shared by multiple entities making personnel requirements of CIP-004-5 extremely onerous. Physical security costs will probably be the biggest component of spending for compliance. It would be best if only certain areas of the facility (i.e. those with cyber assets) be protected, not the whole asset. Recommend drafting a definition based on impact to BES for transient devices and categories for device types. Recommend that the SDT develop a new standard that will allow this one standard to have an implementation date later than the other Version 5 standards. Recommend that the SDT develop a new standard to address communication networks that will allow this one standard to have an implementation date later than the other V5 standards.
Individual
Antonio Richmond
CPS Energy
Yes
No
No
Individual

Michael Falvo
Independent Electricity System Operator
Yes
No
No
Individual
Greg Froehling
Rayburn Country Electric Cooperative
Yes
No
Yes
Comments: Although it may not seem apparent since the focus has been on Medium and High implementation. It is important to note there is no implementation period identified for newly identified Low BES Cyber Assets. With uncertainty around Low BES Cyber Asset determination I feel it would be prudent to identify this situation and assign a period to develop cyber security policies where none may have existed before. The situation could arise during an audit when it is asserted by the entity that they have no Low BES Cyber Assets and the auditor disagrees… at that point it could be a potential violation unless there is a period of implementation to develop cyber security policies. Keeping in mind that FERC allowed an additional year for the Low BES Cyber Assets to develop and implement cyber security policies, I suggest using the timeframe for newly identified medium and high and adding time as the original FERC approved effective date for CIP V5 did.
Individual
Roger Paschall
Texas Reliability Entity
No
I think the Standards Drafting Team should have the flexibility to reduce ambiguity and enhance clarity in any of the existing CIP v5 requirements. There is a significant amount of ambiguous language in CIP v5 and any lessening of that ambiguity can only increase reliability of the BES.
No

Yes
The SAR is focused on the actions of ten people from utilities and three NERC staff members whose SDT performance is a part-time function from their existing suite of responsibilities but whose actions can impact the entirety of the Bulk Electric System and most of the North American general public. That's a lot of responsibility to give to part-timers and expect a world-class product in less than twelve months. I think the SDT should be increased for this specific project by at least an additional eight people, one from each Regional Entity. Personnel from the Regional Entities are independent and cannot be perceived as working for the benefit of the utilities themselves.
Individual
Thomas Foltz
American Electric Power
Yes
No
Yes
Identify, assess, and correct wording modifications: AEP does not have concerns with the removal of the “identify, assess, and correct” language. This wording can be removed and effectively handled by the Reliability Assurance Initiative and the Find, Fix and Track process as necessary. Security controls for Low impact assets: AEP does not believe it is in the best interest of the industry to prescribe security controls for Low impact assets at this time. FERC presented NERC with 4 options for addressing security controls for Low impact assets. AEP recommends NERC request FERC to allow the ERO to conduct a study during the NERC transition study or CIP Version 5 transition program to assess the cyber security programs documented and implemented by entities with Low impact assets. This would provide NERC the visibility needed to determine if specific cyber security controls, a more refined list of criteria for cyber security programs, or industry guidance would help to improve the cyber security posture of Low impact assets. Many entities will be implementing cyber security programs for the first time under CIP version 5 over thousands of assets. These assets will vary in complexity from computer or server in a controlled room environment to protective relays or single loop controllers located in large open areas. The industry will need time to refine their security programs around the varying locations. If more prescriptive controls are written for Low impact BES Cyber Systems the implementation plan should be revised accordingly to allow industry appropriate time to achieve the controls. Communications network: AEP is concerned that the scope and cost of compliance with the NERC CIP standards could increase significantly with little improvement in reliability to the BES if the definition of communications networks and security controls associated with those networks is not addressed properly. NERC should consider the guidance provide by industry in the NERC led technical conferences on 1/21/2014 and 1/23/2014: 1. Consider the risk the

communications network poses to the BES a. This should not be a one-size fits all. Communications networks that present a greater risk should require increased security. 2. Exclude external networks not owned or operated by the entity (e.g. Telecommunications company owned leased lines) 3. Excluding signaling communications (e.g. 4-20 mA, differential voltage, and contact closures) 4. Consider where the communications network resides: a. Does it reside in a control center? b. Does it reside in a generation facility? c. Does it reside in a transmission facility? d. Does it traverse public areas? 5. Review the standards and physical security controls FERC mentioned: a. NIST sp800-53 rev3 control PE-4 b. ISO-27001 control A.9.2.3 c. locked wiring cabinets, disconnected or locked spare jacks, or protection of cabling by conduit or cable trays 6. Avoid complex technical issues like encryption. This technology is difficult to implement in control system environments and may have adverse reliability impacts if implemented incorrectly. Transient Devices: AEP is concerned with the Commission's decision to require security controls for transient devices. The target of the NERC CIP standards should be the BES Cyber Systems. The NERC CIP requirements protect the BES Cyber Systems through a defense in depth strategy that includes cyber security programs, awareness and training programs, physical security, remote access control, local access control, security patch management, malware prevention, cyber security incident response programs, and etc… A standard that requires a similar set of security controls for transient devices would be difficult for an entity to prove compliance with in an audit. By definition transient devices are not connected for an extended period of time to cyber systems where they can be monitored and logged this would prevent the proper documentation of compliance evidence for an audit. AEP requests NERC to revisit the transient devices with FERC to address the auditability concerns and highlight the fact that existing security controls that are required by CIP-003 through CIP-011 will adequately address the security concerns posed by transient devices.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
No
Yes
ATC recommends the following for consideration by the Standards Drafting Team:• Modify the text in the last paragraph of the SAR 'Detailed Description' section to consider input from the industry regarding obvious modifications or finite errors that should be made to the CIP standards while they are 'open' for revision. ATC recommends to modify the last paragraph to read: "When developing these new or modified CIP standards, the SDT may consider input from CIP version 5 transition activities, such as from the NERC transition study or CIP Version

5 transition program, including input from the industry regarding obvious modifications (e.g. typographical errors, vital clarifications, or clear contradictions).”
Group
NERC Standards Review Forum
Russ Mountjoy
Yes
No
Yes
The MRO NSRF recommends that NERC allow flexibility in the schedule and place priority on responding to the directives related to the “identify, assess, and correct” language and communication networks by February 3, 2015. While an approach and subsequent filing that addresses all four FERC directives is preferred, it might not be feasible given the complexity of the issues. Consider modifying the text in the last paragraph of the ‘Detailed Description’ section to also give the SDT the option of considering input from the industry regarding obvious modifications that should be made to the CIP standards while they are ‘open’ for revision. Obvious modifications could include typographical errors, crucial clarifications, and the correction of clear contradictions. Since the input is informal, the SDT would not be obligated to consider the input or provide any justification for its rejection. We suggest revised wording to read, “When developing these new or modified CIP standards, the SDT may consider input from CIP version 5 Transition activities, such as from the NERC transition study or CIP Version 5 transition program. Include informal input from industry regarding obvious modifications (e.g. typographical errors, vital clarifications, and clear contradictions).”
Group
WECC
Steve Rueckert
Yes
No
No
Individual
Judy VanDeWoestyne
MidAmerican Energy Company

Yes
No
No
Individual
James Gower
Entergy
No
Comments: 1.)Modify or remove the “identify, assess, and correct” language in 17 CIP version 5 requirements. Response: Entergy supports entities ability to have the flexibility to correct self-identified issues that have minimal to no impact on the Bulk Electric System, such as documentation issues, and believes this language should remain in the standards. 2.)Develop modifications to the CIP standards to address security controls for Low Impact assets. Response: Applying security controls at Low Impact assets would have virtually no practical risk reduction value and would be done purely for the perceived benefit. 3.)Develop requirements that protect transient electronic devices. Response: Entergy’s position is that transient devices are not assets that comprise the Bulk Electric System, and therefore are outside the scope of the NERC CIP standards. Any risk these devices pose is already mitigated by compliance with the existing CIP standards for cyber assets that are within NERC CIP scope. 4.)Create a definition of “communication networks” and develop new or modified standards that address the protection of communication networks. Response: No comments
No
No
Individual
Nazra Gladu
Manitoba Hydro
Yes
No
Yes

(1) Manitoba Hydro is of the view that including IAC language in the text of NERC reliability standards may create confusion regarding the duty to comply and introduce conflicts with North American legislation imposing an obligation to comply with NERC standards. Thus, Manitoba Hydro supports the removal of the IAC language. Therefore, Manitoba Hydro believes that the option to modify the IAC language should be eliminated from the SAR. In the January 8th, 2014 letter from F. Gorbet on behalf of the NERC BOT to John Anderson of the MRC requesting policy input to the BOT, Gorbet states that “NERC supports drafting team removal of the IAC language…”. The SAR should be revised accordingly. (2) The word “Low Impact” is not defined in the NERC Glossary of Terms, and as such should be defined, or de-capitalized. (3) Detailed Description, first bullet - add quotation marks around the phrase “identify, assess, and correct” for consistency with the rest of the SAR.
Individual
Bill Temple
Northeast Utilities
Yes
No
Yes
1. Modify or remove the “identify, assess, and correct” language in 17 CIP version 5 requirements. Northeast Utilities recommends removing this language from the standards. These activities are more appropriate for enforcement activities or events analysis. 2. Develop modifications to the CIP standards to address security controls for Low Impact assets. Northeast Utilities recommends the SDT develop a new standard that will allow this one standard to have an implementation date later than the other V5 standards. Low Impact assets, like substations, are often shared by multiple entities making personnel requirements of CIP-004-5 extremely onerous. Physical security costs will probably be the biggest component of spending for compliance. It would be best if only certain areas of the facility (i.e. those with cyber assets) be protected, not the whole asset. 3. Develop requirements that protect transient electronic devices. Northeast Utilities recommends drafting a definition based on impact to BES for transient devices and categories for device types. NU recommends that the SDT develop a new standard that will allow this one standard to have an implementation date later than the other V5 standards. 4. Create a definition of “communication networks” and develop new or modified standards that address the protection of communication networks. Northeast Utilities recommends that the SDT develop a new standard to address communication networks that will allow this one standard to have an implementation date later than the other V5 standards.
Individual
Tracy Richardson
Springfield Utility Board

Yes
No
No
Individual
Clifford Johnson
Consumers Energy
No
Items 2 and 3 of this SAR do not have a timeframe for completion and provide no additional direction or goal for the outcome. For item 2, entities do not require a detailed list of controls to develop the required policies. Entities are more than capable of utilizing cyber security best practices and the requirements laid out in CIP-003 through CIP-011 as guidelines or starting points for developing the policies required for the lower, and in some cases virtually zero impact assets. CIP-003-5 R2 lists specific subjects that must be covered. These are cyber security awareness, physical security controls, electronic access controls (external routable and dialup) and incident response. These basic requirements are adequate direction for entities to proceed. There is no need for greater, more prescriptive details. Additionally, the “policy” development requirement is highly appropriate due to the somewhat “catch-all” aspect of the Low Impact category. These security controls will apply to hundreds, if not thousands, of Low Impact devices often in remote, unmanned locations and the importance and reliability impact of these will vary greatly. The volume of Low Impact assets make further prescriptive requirements unmanageable and causes substantial regulatory burden. Many of the Low Impact assets will have no external connectivity whatsoever. At most if not all entities, these assets are either located in locked cabinets or located in locked buildings inside fenced and locked substations. In addition to the low impact, (if not nearly-zero in many cases), the overall risk (threat, vulnerability, cost/impact) of/to these assets is in general, negligible. Again, modification to the CIP standards to address security controls for Low Impact assets could add complexity, if requirements beyond policy development are mandated. Item 4 has the potential to create significant undue burden on entities. In general, much of the communication systems utilized today are over public carrier where entities have extremely little control beyond negotiated service level agreements and virtually no way of validating if the carriers are securing these systems from day-to-day. It would seem more appropriate, that requirements for these systems be included in other, yet-undeveloped CIP standards, or a new set of standards specifically addressing these types of systems. In either case, these other standards should be specifically applicable to these telecommunications carriers as well.
No

No
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
No
Yes
1) NERC needs to clearly address, with justification, specific implementation timeframes/deadlines within this SAR. The initial CIP V5 standards were approved by the industry with effective dates that were directly associated with the scope of work prescribed by CIP V5, as written at the time of proposal. This SAR will introduce new standards and/or enhance the current CIP V5 standards, thereby increasing the prescribed work scope (and potentially require re-work). Additionally, resources that are focused on CIP V5 implementation will now have additional workload in order to participate in the Standards Development Process associated with this SAR. This was not anticipated when the initial CIP V5 effective dates were approved by the industry; therefore, the CIP V5 effective dates must be revisited given the extent of change with 17 requirements being modified (IAC removal) and new requirements (and potentially new standards) being promulgated. These new requirements (and standards) will affect the current requirements being implemented. 2) NERC needs to provide guidance to the industry on how to handle Low Impact BES Cyber Systems (and communications networks) while this SAR is being developed. Due to the aggressive implementation dates specified in CIP V5, the industry cannot wait to work on applying security controls to their Low Impact Assets. This SAR will develop a set of security controls that must be applied to Low Impact BES Cyber Systems. The current CIP V5 standards allow each entity to define their own security controls to address broad subjects. NERC needs to promote consistency in implementation by providing the industry an extension on Low Impact Assets and communications networks that coincides with the development this SAR, so that a defined set of security controls can be developed and then implemented by the industry. 3) NERC needs to include in this SAR a provision whereby NERC must provide timely guidance to the industry on how the CIP V3 to CIP V5 transition is to take place. NERC must also provide implementation time leeway, per the Transition Study, for entities to migrate from V3 to the modified V5.
Group
Duke Energy
Michael Lowman

Yes
No
Yes
(1) Duke Energy would like for the drafting team to consider creating separate standard(s) and requirements that address security controls for Low Impact Assets. We believe this would better simplify the monitoring and enforcement process. (2) We ask the SDT to clarify the meaning and intent of protecting transient electronic devices. Is the intent to protect the transient devices themselves or the devices that connect to those identified transient devices? (3) When developing a definition of communications network and determining what to protect, the SDT should ensure that “integrity, confidentiality, and availability” are maintained as principles in the development. (4) In the development of the scope and definition of communication networks, we would like the SDT to consider the following items: a. Identify the ownership line of demarcation for compliance when multiple Owners are involve such as i. Vendors ii. Other Registered Entities iii. Wireless iv. ESPs v. Point-to-point networks vi. Logical vs. Physical networks vii. encryption/VPN communications viii. trusted vs. non-trusted networks b. further break down of the definition to include: i. entity-owned ii. intra-entity iii. vendor-owned iv. Analog v. serial-to-fiber vi. TCP/IP fully enmeshed
Individual
Ayesha Sabouba
Hydro One
No
The SDT should provide a definition for "transient electronic devices".
Yes
The Ontario Energy Board is also looking at cyber security requirements for utilities within Ontario, Canada. I am not sure how far they have progressed, however.
No
Individual
Steve Karolek
We Energies d/b/a Wisconsin Electric Power Company
No
While we understand NERC’s desire to make progress on all of FERC’s Order 791 directives, it is important to ensure that resources are focused first and foremost on those which are time-bound and that those directives not due in one year should not be worked on to the detriment of doing a good job addressing those which are due in one year. FERC recognized the sensitivity and complexity of these areas when they chose to not put a time box on

them. As an industry we need to make sure we spend the appropriate time considering and addressing these issues.
No
Yes
* As the drafting team “considers whether any further standard protections are needed to address potential vulnerabilities associated with transient devices (e.g., thumb drives and laptop computers)” they should remember that thumb drives are not themselves Cyber Assets/Systems and the need may be less to protect thumb drives than to protect Cyber Assets/Systems from thumb drives. Additional protection for information on thumb drives may also be in order but that falls in the realm of information protection not transient device protection. Thumb drives should not be considered to be transient devices. * The applicability section (4) should be updated to remove section 4.2.2 for the reasons previously documented by We Energies’ Howard Rulf and also should be updated to specifically exempt small distributed generation with aggregated capacity less than 75MW (e.g. individual wind turbines). [Howard Rulf’s previously documented comments: Section 4.2.2 wording means that for all entities other than DP, the standard applies only to their BES Facilities. A BES Facility is essentially equipment operating at >100 kV that is connected to the BES by terminals. Nothing in a Control Center is >100 kV connected to the BES by terminals. These standards will only apply to entity functions that own equipment operated at >100 kV and are connected by terminals (i.e. generators, transmission lines, high voltage transformers, etc.).]
Individual
Richard Vine
California ISO
Agree
IRC's Standards Review Committee
Individual
Chris Scanlon
Exelon
No
Under Industry Need, item #1: “Modify or remove the “identify, assess, and correct” language in 17 CIP version 5 requirements.” Removal of the “identify, assess, and correct” (IAC) wording without any replacement wording to promote compliance enforcement maturity that allows very strong programs with very minor variances to be compliant is problematic. The IAC language was essential for entities to support approval of the CIP Version 5 Standards. While FERC Order 791 requests that compliance language be removed from the requirements, the IAC language in the requirements may need to be replaced with language elsewhere in the Standards, such as in the Measures, to reflect the underlying purpose of the IAC language. Proposed Revision: “Modify or replace the “identify, assess,

and correct" language in 17 CIP version 5 requirements."Under Industry Need, item #3: "Develop requirements that protect transient electronic devices." The scope needs clarification. Protecting transient devices should not be the focus of this activity, but rather protecting the Bulk Electric System reliability from risks that may be introduced by use of a transient device. While protecting the Bulk Electric System would likely include some controls on the transient devices to avoid risk to BES Cyber Systems and the Bulk Electric System, focus of the controls and other potential requirements will be better designed with the proper scope wording that does not focus protection on the transient assets. Proposed Revision: "Develop requirement(s) that protect the Bulk Electric System reliability where transient electronic devices (not classified as BES Cyber Assets as described in BES Cyber System definition) are used." Note For Reference the BES Cyber System Definition - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.) Detailed Description, bullet #3: "The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP Standards." This action may create a timing problem for the SDT. Ideally, the SDT will work on all four Directive areas concurrently, to the degree possible, and the SDT may be able to address the issues identified within Order 791 before the survey results are available. Proposed Revision to the last sentence of the bullet: "The SDT shall review information from this survey, as available during the Standards development process, for relevant and timely insight to the development of new or modified standards associated with transient devices."Detailed Description, bullet #4: "The SDT shall review the technical conference testimony and comments to inform the development of the definition for communication networks and a new or modified standards for the protection of communication networks." Again, this may create a timing issue for the SDT. Order 791 directs a one year timeframe for communication networks, thus requiring the SDT to move quickly on the development work. Recognizing that this is a FERC led conference and not controlled by NERC, the action item should allow for flexibility. Proposed Revision to the last sentence of the bullet: "The SDT shall review the technical conference testimony and comments as available during the Standard development process for relevant and timely insight to the development of new or modified standards for the protection of communication networks."Definitions are part of the Standard: It may be useful to include a note in this SAR stating that a modification to a CIP definition(s) is considered a modification to a Standard. This would clarify that if an issue can be addressed with only a change to a definition that would be acceptable under this SAR. VRF/VSL: If the SDT will be working on revisions to the VRF &/or VSLs that should be stated in the SAR. Language Tweaks: Industry

Need: to clarify that the SAR language summarized the Order 791 directive details, consider adding that note as follows: On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards, and also directed that NERC make the following modifications to those standards (as summarized from FERC Order 791): Industry Need Typo: Last sentence in the Industry Need section, “time frame” should be one word as it is later in the Detailed Description. Brief Description: While it may be unlikely, the SAR should not preclude use of another standard or standard revision to address a FERC directive. For instance, a standard for protection of communication networks could fall within the COM standards family. Consider including the added phrase to read as follows: “The proposed project will develop new or modify existing requirements in the CIP standards, or other NERC Reliability Standards if determined the best approach, to address the directives from FERC Order No.791. This project may also consider input that may be provided from CIP version 5 transition activities, for example from the NERC transition study or CIP Version 5 transition program.”Detailed Description: The description should further emphasize that the scope of SDT work is to address those concerns raised in Order 791. Please consider including the added phrase to read as follows: “As stated above, the purpose of the proposed project is to respond to the directives in the FERC Order 791 and to respond within a timeframe required by the order for the directives related to “identify, assess and correct” language and communication networks. The following is a description of the responses the standard drafting team (SDT) shall consider during development of new or modified standards to address the concerns raised in Order 791: …”Detailed Description: In the fourth bullet, the first sentence is missing a word and “communications” should be singular: “The SDT shall consider how to define the term “communication networks” and develop new or modified …”
No
No
Individual
Michael Haff
Seminole Electric Cooperative, Inc.
No
Seminole agrees with comments provided by the National Rural Electric Cooperative Association (NRECA).
No
Yes
Seminole agrees with comments provided by the National Rural Electric Cooperative Association (NRECA). In addition, Seminole believes that two separate issues (transient

devices and definition of BES Cyber Asset) have been inappropriately combined and should be addressed separately. Seminole supports the survey to identify the 15-minute parameter issues for FERC. Seminole believes that separation of these two issues would allow the following: 1. An independent review of the 15 minute parameter; and 2. A determination of what should qualify as a transient device, and what controls should be put into place for those devices It will be difficult to combine the 15 minute standard and transient devices directly. Any device plugged into the ESP will need to be a Cyber Asset because misoperation or malware would have the ability to impact the Facility within 15 minutes. The 30-day window goes away other than the parenthetical footnote in the definition. That was FERC's objection. Combining two separate issues in this way confuses the matter that the team was directed to address in Order 791.
Individual
Amelia Sawyer
CenterPoint Energy
No
The following statements on page 3 of the SAR exceed what is directed in Order 791:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."Paragraph 124 of Order 791 directs "NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition." CenterPoint Energy recommends deleting the statements, ""During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards." as the statements and survey are not related to the currently directed modifications or activities of the SDT. Based on Order 791, the directed survey and its results are for an informational filing and future consideration by the Commission. Using the survey results to inform the development of the new or modified standards may add an unnecessary level of complexity, frustrate the process, and delay the final deliverable.
No

No
Group
Electric Reliability Compliance
Josh Andersen
Yes
No
Yes
CIP-008 - Requirement R1. Part 1.1 : Salt River Project recommends that NERC develop the standard classification for identifying Cyber Security Incidents. Because this is left up to each entity, it leaves room for discrepancy. Therefore there could be an inconsistency in classification and reporting amongst the industry entities. Additionally, by creating a standard and consistency, entities would be able to better collaborate in prevention, detection and eradication methods to protect the bulk electric systems. CIP-011 – General Note : While the development of requirements for Low Impact Cyber Systems might be on the roadmap as part of the larger effort to address security controls for these systems, Salt River Project recommends that NERC either provide specific information protection requirements for Low Impact BES Cyber Systems or exclude them from the requirements.
Individual
Michelle R. D'Antuono
Occidental Energy Ventures Corp.
No
Occidental Energy Ventures Corp. (“OEVC”)agrees that the SAR captures FERC’s primary intent in Order 791. In addition, we are aware of the limited time frame that has been given to NERC and the industry to address several of the rulings. Unfortunately, the Commission’s directive to eliminate the risk-based qualifier in 17 requirements eliminates one of the major reasons why we voted to approve CIP Version 5 to begin with. However, our reading of Order 791 indicates that FERC is willing to accept other equally effective alternatives to the “identify, assess, and correct” language. As such, we found it disheartening that the SAR drafting team seems to propose a solution which mostly involves the education of stakeholders by ERO Compliance and Enforcement staff. In OEVC’s view, this is not sufficiently binding to those organizations – who will be free to change their oversight approach as they see fit. We are not suggesting that NERC or the Regions will make alterations lightly, but our experience of the CAN process and other similar initiatives has been that they are not rigorous enough. We ARE suggesting that the SAR must be updated to capture the goal that a definitive and binding review/acceptance compliance process

must be developed. In fact, the NERC Rules of Procedure may be a candidate. It was updated to allow for individual exceptions to allow appeals related to the Definition of the BES – a project that was at least as complex and controversial as this one is.
No
Yes
The focus of the CIP v5 revisions initiative must be placed on the two items that FERC has assigned a due date (remove the “identify, assess, and correct” language and address communication networks). In OEVC’s view, both of these are substantial modifications that deserve the development team’s full attention. This means that the remaining two items (create security controls for Low Impact assets and requirements that protect transient electronic devices) should be deferred to Phase II of the project. We recommend that the SAR be updated to reflect this realistic development approach.
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
No
NRECA’s comments focus on ensuring the SAR accurately represents the FERC directives in Order No. 791. In the “Industry Need” and “Detailed Description” sections the following revisions should be made: (1) the language used in the SAR for Low Impact assets should be revised to remove references to security controls specificially, and replaced with “……address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity’s protections for Low Impact assets”; (2) the language used in the SAR for transient devices should be revised to say “…….develop either new or modified standards to address the reliability risks posed by connecting transient devices that fall outside the BES Cyber Asset definition to BES Cyber Assets and Systems”; (3) the language used in the SAR for communications networks should be modified to state that the focus is on nonprogrammable components of communication networks; and (4) the language in the first line of the last bullet under “Detailed Description” should be revised to state “Create a definition of “communication network”……..”
No
Yes
What role will the SDT have in developing the survey for transient devices? The SDT should collaborate with NERC to develop the survey and this should be stated in the SAR. The SAR should make reference to the forthcoming order on clarification and rehearing and state that the SDT will factor this in to their work.
Group
ACES Standards Collaborators

Trey Cross

Yes

(1) We support NERC's efforts in modifying the NERC CIP Version 5 Standards to address FERC directives regarding "identify, assess, and correct (IAC)" language, Low Impact requirements, protection of transient devices, and communication network definitions. Removal of the IAC language will eliminate uncertainty of auditing the requirements that contain this language. Any standard or requirement should have clear, concise, and auditable language that is consistently applied across all NERC regions. (2) However, the implementation plan is unclear. Are registered entities going to have to comply with the current IAC language before it is modified since the standards are approved? We ask that the SAR drafting team consider these implementation issues and provide guidance during the development of this standard.

No

Yes

(1) We are concerned that modifying the 'IAC' language will delay version 5 implementation efforts for internal controls and would like NERC to provide guidance how to build internal controls based upon the Reliability Assurance Initiative (RAI) as soon as possible. Specifically, guidance needs to be provided for those requirements that relate to low impact BES Cyber Systems and high frequency violated requirements that IAC was written to address. Without the IAC language, the CIP version 5 standards could result in zero defect compliance for each deviation from a requirement. We support NERC's focus on internal controls and would like to see formal guidance issued during the interim period while this drafting team is revising the version 5 standards. We appreciate that NERC has stated publicly that they are committed to a non-zero defect policy and are hopeful the implementation studies and transition guidance will provide ultimate clarity around this issue. (2) As addressed in question 1, we support NERC's focus on standards that are clear, concise and auditable. The Version 5 Standard Drafting Team wrote the current Low Impact requirements in a non-prescriptive manner to allow for entities that do not currently have Critical Assets as defined in CIP Version 3 to build a customized compliance program based on the limited risk they pose to the Bulk Electric System. We support NERC's effort to allow small entities the flexibility to interpret those requirements that match their infrastructure, resources and program size; however, that flexibility must also be consistently audited across all regions. NERC should develop requirements that provide small entities and auditors a baseline of compliance to remove the possibility of differing interpretations of compliance for the Low Impact requirements. (3) Regarding the FERC directive that addresses requirements for transient devices, we understand that this is a complicated issue with many questions that need to be answered, e.g., "what is the definition of a transient device, what are the time requirements that qualifies a device to become a transient device, is a laptop considered a transient device, etc. Given the spectrum of devices, timing and other considerations for cyber assets to be a possible transient device, we recommend that any definition of a

transient device includes supporting documentation that provides examples of what is and what is not considered a transient device to remove any uncertainty. (4) ACES recommends that NERC use an industry definition of network communication in order for entities to leverage existing standards, definitions, and network configurations. NIST 800-82 has been industry vetted and written specifically for industrial control systems (ICS). Their definition of a control network is: “Those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.” Furthermore, standard requirements written for communications networks need to have clear boundaries about what is included and what is not included. What is included must be under the registered entity’s control. For example, this cannot become a standard that requires a registered entity to ensure the communications infrastructure of their telecom provider is CIP compliant. In other words, the standard cannot become a national or international telecommunications infrastructure standard. (5) We support the use of this definition in that is specifically speaks to ICS functionality, assets and cyber asset that run a facility.
Group
Bonneville Power Administration
Andrea Jessup
Yes
No
No
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
Yes
No
AZPS does not have familiarity with any Canadian provincial regulatory
No
The thoughtful implementation of new or revised standards is just as critical as the content of the standards themselves. Therefore, AZPS urges the Standards Drafting Team to ensure that any new or modified standards are also accompanied by a transition and/or implementation timeline that best matches the magnitude of the proposed changes. Bearing in mind those entities with a large number of BES assets may need more time to implement

any associated changes than entities with relatively few BES assets. AZPS is appreciative of NERC's efforts on the CIP Version 5 Implementation Pilot program and thus requests that the lessons learned from those pilots be considered by the drafting team as it develops modifications to the CIP standards. Incorporating lessons learned now will yield valuable perspective and may prevent rework later. In addition, AZPS further urges the SDT to be mindful of not only the technical aspects of the modifications to the standards but also the auditability of control effectiveness as applied to the intent of the standard. Doing so would help to ensure the technical processes are sufficiently clear and can also be easily documented – both of which are of critical importance. Lastly, AZPS is supportive of NERC's efforts with respect to the Reliability Assurance Initiative and its movement away from the "zero tolerance" approach. AZPS requests that NERC and the standards drafting team make modifications or develop an approach the can be consistently applied across all NERC standards.
Individual
Kenn Backholm
Public Utility District No.1 of Snohomish County
No
Recommend modifications to the SAR language to clarify and align with FERC order 791: SAR, page 3:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."• Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices.• Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR. Recommends the following be considered: i) Suggest changing the Detailed Description's second bullet to The SDT shall consider the development of necessary Standard modification or new Standards that address security controls for Low Impact assets. ii) Suggest splitting the Detailed Description's third bullet into two bullets for clarity. Replace this third bullet with the following a - c. a) The SDT shall consider how to define the term transient device. b) The SDT shall consider whether further Standard protections are needed to address vulnerabilities associated with transient devices. c) The SDT will review the results of the ERO survey concerning the use of the "15 minute" parameter to inform the SDT's development of a new / modified Standards for the protection of Cyber Assets and BES Cyber Systems from the vulnerability introduced by transient devices.
No

Yes
NERC staff requested that the industry not submit Requests for Interpretation (RFI). However, more detailed reviews of the approved CIP Version 5 Standards generated additional questions regarding compliance. NPCC members are requesting a process for seeking clarifications so that company implementation expectations of CIP Version 5 will be consistent with future audit expectations. Recommend removing the “identify, assess, and correct” language in 17 CIP Version 5 requirements. Recommend that the Standard Drafting Team develop a new standard that will allow this one standard to have an implementation date later than the other Version 5 standards. Low Impact assets, like substations, are often shared by multiple entities making personnel requirements of CIP-004-5 extremely onerous. Physical security costs will probably be the biggest component of spending for compliance. It would be best if only certain areas of the facility (i.e. those with cyber assets) be protected, not the whole asset. Recommend drafting a definition based on impact to BES for transient devices and categories for device types. Recommend that the SDT develop a new standard that will allow this one standard to have an implementation date later than the other Version 5 standards. Recommend that the SDT develop a new standard to address communication networks that will allow this one standard to have an implementation date later than the other V5 standards. Recommend clarifying the applicability of CIP-002-5. Registered Transmission Operator (“TOP”) are automatically classified as a medium impact through application of Attachment 1, however some registered TOPs do not have any BES Cyber Assets under the Definition: “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.”Through registration and application of section 2.12 of Attachment 1, a TOP is automatically selected to the medium impact rating; however some registered TOPs may not have any BES assets that can impact the reliable operation of the BES. Based on discussion with subject matter experts at NERC and WECC there appears to be confusion on how to address this issue. In addition to clarifying CIP-002-5, it would be helpful for NERC or the Regional Entities to review or validate Registered Entitles CIP-002-5 assessment prior to the version 5 implementation so the RE has time to address CIP v5 requirements. Although there is an implementation plan, it is clear that going from no Critical Assets in CIP v3 & v4 to a medium impact will require significant funds, resources, and schedule.
Individual
paul haase
seattle city light
No
Regarding following language: “During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the “15-minute” parameter. The SDT shall

review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards." Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices. Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR.
No
No

Additional Comments:

Idaho Power
Molly Devine

1. No
Comments:

The scope of the SAR should be expanded to include a revision to the CIP-002-5.1 standard that will clarify the process that should be followed to identify BES Cyber Systems. The CIP-002-5.1, standard as currently written, creates a great deal of confusion and uncertainty around how to proceed or how to maintain compliance with the standard.

2. Yes
Comments:

In order to successfully implement any new requirements surrounding communications networks that connect Canadian and US utilities one of two options must be used. 1. The connections between the utilities must be exempted from requirements or 2. the Canadian provinces must implement the same requirements. For example if a new requirement that is approved that involves encrypting communication data over a communications link that is physically crossing the international border between a Canadian utility and a US utility but is only required by the US utility. Only requiring the US utility to implement encryption on the communications link while not requiring the Canadian utility to do the same will create many difficulties, challenges and confusion. Additionally, the cost and implementation details may be contentious to the Canadian utility and leave both utilities in a bind of how to implement and support systems that are deemed "critical".

3. Yes
Comments:

The development of standards surrounding communication networks needs to be done carefully and clearly as these topics start to touch upon issues that have previously been excluded from the CIP standards and will need to be fully vetted. NERC should consider defining different regulations for utility owned communications versus leased facilities from external entities. Each of these two scenarios pose separate challenges and risks and need thoughtful consideration taking into account the fundamental differences of what is in the utility's control and what can and will need to be addressed with external providers. Additionally, there is no single reliability standard that addresses "communications networks". Instead, the various communications network requirements are sprinkled throughout the NERC reliability standards (e.g. COM, PRC, TOP, CIP, etc.). There should be an effort made to have a consolidated standard (or set of standards) for "communications networks" owned by Functional Entities. There is also a great deal of concern over the appearance that NERC's seems to be viewing the only option as removing the "identify, assess, and correct" language rather than considering other options. Although, there has been more communication as of late about the RAI there needs to be a more concerted effort to move away from the zero-defect approach in some fashion to allow the entities to protect and not just comply.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, please email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the Bulk-Power System through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Cyber Security Standards		
Date Submitted:	Original: January 15, 2014 Revised: March 17, 2014		
SAR Requester Information			
Name:	Ryan Stewart		
Organization:	NERC		
Telephone:	404-446-2569	E-mail:	Ryan.Stewart@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard ☒ Revision to existing Standard		☒ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.
Industry Need (What is the industry problem this request is trying to solve?):
On November 22, 2013, FERC issued Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*. In this order, FERC approved the new and modified CIP standards, commonly

SAR Information
referred to as the CIP Version 5 standards, and directed that NERC make the following modifications to those standards: 1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements. 2. Develop modifications to the CIP standards to address security controls for Low Impact assets. 3. Develop requirements that protect transient electronic devices. 4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks. FERC directed NERC to submit new or modified standards responding to the directives related to the "identify, assess, and correct" language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time-frame for NERC to respond to the Low Impact and transient electronic devices directives.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The proposed project will develop new or modify existing requirements in the CIP standards to address the directives from FERC Order No. 791. This project may also consider input that may be provided from CIP version 5 transition activities, for example from the CIP Version 5 transition program.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
As stated above, the purpose of the proposed project is to respond to the directives in FERC Order No. 791 and to respond within the timeframe required by the order for the directives related to the "identify, assess, and correct" language and communication networks. The following is a description of the responses the standard drafting team (SDT) shall consider during development of the new or modified standards: • The SDT shall work to remove or modify the identify, access, and correct language. The SDT shall work with NERC compliance and enforcement staff to inform and educate stakeholders on the development of alternative approaches for accomplishing the goals underlying the inclusion of the identify, assess, and correct language without placing compliance language in those requirements. • The SDT shall consider the necessary standard modifications to be developed that address the lack of objective criteria for Low Impact assets.

SAR Information
• The SDT shall consider the necessary modifications to the CIP standards to address protections related to potential vulnerabilities associated with transient devices. • The SDT shall consider how to define the term "communication networks" and develop new or modified standard(s) that address the Commission's concerns for the protection of communication networks. When developing these new or modified CIP standards, the SDT may consider input from CIP version 5 transition activities, for example from the CIP Version 5 transition program. The SDT may also consider information from the survey NERC is directed to conduct on the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.

Reliability Functions		
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected Bulk-Power Systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected Bulk-Power Systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected Bulk-Power Systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected Bulk-Power Systems.
☒	6. Personnel responsible for planning and operating interconnected Bulk-Power Systems shall be trained, qualified, and have the responsibility and authority to implement actions.

Reliability and Market Interface Principles	
☒	7. The security of the interconnected Bulk-Power Systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation
CIP-002-5.1	BES Cyber System Categorization
CIP-003-5	Security Management Controls
CIP-004-5.1	Personnel & Training
CIP-005-5	Electronic Security Perimeter(s)
CIP-006-5	Physical Security of BES Cyber Systems
CIP-007-5	Systems Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-5	Recovery Plans for BES Cyber Systems
CIP-010-1	Configure Change Management and Vulnerability Assessments
CIP-011-1	Information Protection

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
ERCOT	None
FRCC	None
MRO	None
NPCC	None
RFC	None
SERC	None
SPP	None
WECC	None

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, please email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the Bulk-Power System through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Cyber Security Standards		
Date Submitted:	Original: January 15, 2014 Revised: March 17, 2014		
SAR Requester Information			
Name:	Ryan Stewart		
Organization:	NERC		
Telephone:	404-446-2569	E-mail:	Ryan.Stewart@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.
Industry Need (What is the industry problem this request is trying to solve?):
On November 22, 2013, FERC issued Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*. In this order, FERC approved ~~version 5 of the~~the new and modified CIP standards,

SAR Information
commonly referred to as the CIP Version 5 standards, and ~~also~~ directed that NERC make the following modifications to those standards: 1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements. 2. Develop modifications to the CIP standards to address security controls for Low Impact assets. 3. Develop requirements that protect transient electronic devices. 4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks. FERC directed NERC to submit new or modified standards responding to the directives related to the "identify, assess, and correct" language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any ~~time~~ time-frame for NERC to respond to the Low Impact and transient electronic devices directives.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The proposed project will develop new or modify existing requirements in the CIP standards to address the directives from FERC Order No. 791. This project may also consider input that may be provided from CIP version 5 transition activities, for example from the CIP Version 5 transition program~~, including NERC's transition study or CIP Version 5 transition program~~.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
As stated above, the purpose of the proposed project is to respond to the directives in FERC Order No. 791 and to respond within the timeframe required by the order for the directives related to the "identify, assess, and correct" language and communication networks. The following is a description of the responses the standard drafting team (SDT) shall consider during development of the new or modified standards: • The SDT shall work to remove or modify the identify, access, and correct language. The SDT shall work with NERC compliance and enforcement staff to inform and educate stakeholders on the development of alternative approaches for accomplishing the goals underlying the inclusion of the identify, assess, and correct language without placing compliance language in those requirements. • The SDT shall consider the necessary standard modifications to be developed that address ~~security controls~~the lack of objective criteria for Low Impact assets.

SAR Information
• The SDT shall consider the necessary ~~standards~~ modifications to ~~be developed thatto~~ the CIP standards to address ~~whether any further standard~~ protections ~~are needed to address~~~~from~~related to potential vulnerabilities associated with transient devices ~~(*e.g.*, thumb drives and laptop computers)~~. ~~During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards.~~ • The SDT shall consider how to define the term "communication~~s~~ networks" and develop new or modified standard(s) that address the Commission's concerns for the protection of communication networks. ~~As stated in Order No. 791, FERC staff will lead a technical conference that, among other things, will address the issue of protecting the non-programmable components of communication networks. The SDT shall may review the technical conference testimony and comments to inform the development of the definition for communication networks and new or modified standards for the protection of communication networks.~~ When developing these new or modified CIP standards, the SDT may consider input from CIP version 5 transition activities, ~~such as~~for example from the ~~NERC transition study or~~ CIP Version 5 transition program. The SDT may also consider information from the survey NERC is directed to conduct on the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.

Reliability Functions	
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐ Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐ Market Operator	Interface point for reliability functions with commercial functions.
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected Bulk-Power Systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected Bulk-Power Systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected Bulk-Power Systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected Bulk-Power Systems.
☒	6. Personnel responsible for planning and operating interconnected Bulk-Power Systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected Bulk-Power Systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation
CIP-002-5.1	BES Cyber System Categorization

Related Standards	
CIP-003-5	Security Management Controls
CIP-004-5.1	Personnel & Training
CIP-005-5	Electronic Security Perimeter(s)
CIP-006-5	Physical Security of BES Cyber Systems
CIP-007-5	Systems Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-5	Recovery Plans for BES Cyber Systems
CIP-010-1	Configure Change Management and Vulnerability Assessments
CIP-011-1	Information Protection

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
ERCOT	None

Regional Variances	
FRCC	None
MRO	None
NPCC	None
RFC	None
SERC	None
SPP	None
WECC	None

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements by CIP Senior Manager approval of the policies specified in Part 2.1.

The language in Requirement R2, Part 2.4 "external routable protocol paths" and "Dial-up Connectivity" was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.4 uses the phrase "external routable protocol paths" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. The Standard Drafting Team (SDT) intent in using the phrase "external routable protocol paths" is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).

The additions to Requirement R2, in particular the processes required under Parts 2.2-2.6, address FERC Order No. 791 paragraphs 106-110, which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets. The SDT pulled language and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2.

In FERC Order No. 791 paragraphs 111-112, FERC upheld that creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.

R2. Each Responsible Entity for its assets containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have external routable protocol paths.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These

delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 15	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 16	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 16 calendar months but did complete this approval in less than	calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more processes for	calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 18 calendar months of the previous approval. (2.1) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not reinforce cyber security practices at least quarterly but did reinforce cyber security practices at least every two quarters. (2.6)	or equal to 17 calendar months of the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include two of the topics as	assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include three of the	document or implement any processes for assets with a low impact rating to include the operational or procedural control(s) to restrict physical access as required by Requirement R2, Part 2.2. (2.2) OR The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.5 for assets with a low impact rating in less than or equal to 16 calendar months. (2.6)	required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include one of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security	topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include two of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR	document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity did not implement any Cyber Security Incident response plans for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not implement a security awareness program

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				practices every three quarters. (2.6) OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 in more than 16 calendar months but less than or equal to 17 calendar months. (2.6)	The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 for assets with a low impact rating in more than 17 calendar months but less than or equal to 18 calendar months. (2.6)	for assets with a low impact rating that collectively included the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced cyber security practices at least every 15 months. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced the topics

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						within 18 calendar months as required by Requirement R2, Part 2.6. (2.6)
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but	The Responsible Entity has used delegated authority for actions where allowed by the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of the requirement is to outline a set of protections designed for all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at a programmatic or site level, not an individual device or system level.

There are four main areas that must be covered by this security program: physical security, electronic access controls for all external routable protocol paths or Dial-up Connectivity, a security awareness program, and cyber security incident response plans.

The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary.

2.1 - As with Requirement R1, the number of policies and the specific language used in them would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas in CIP-003-6, Requirement R2, Parts 2.2 through 2.6. The Responsible Entity has flexibility in the number and structure of its policies to meet its needs and organization. Examples include developing a single comprehensive cyber security policy covering these topics for all in-scope assets, several comprehensive cyber security policies based on asset type, or a single high-level umbrella policy with additional policy detail in lower level documents in its documentation hierarchy.

2.2 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.

2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity’s controls.

2.4 – The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. The electronic access controls should address the risk of using the asset’s external connectivity to gain access to the low impact BES Cyber Systems. The entity should be able to describe how its electronic access controls on the external connectivity paths protect the collection of low impact BES Cyber Systems at the site. The intent is to reduce the risk of aggregation of numerous low impact BES Cyber Systems at the site or across multiple sites through external connectivity.

Examples of sufficient access controls may include:

- All the external routable protocol connectivity paths to the asset pass through a firewall that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are shielded from or to the world-wide-web (e.g. IP addresses, ports, services, and data diode) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.

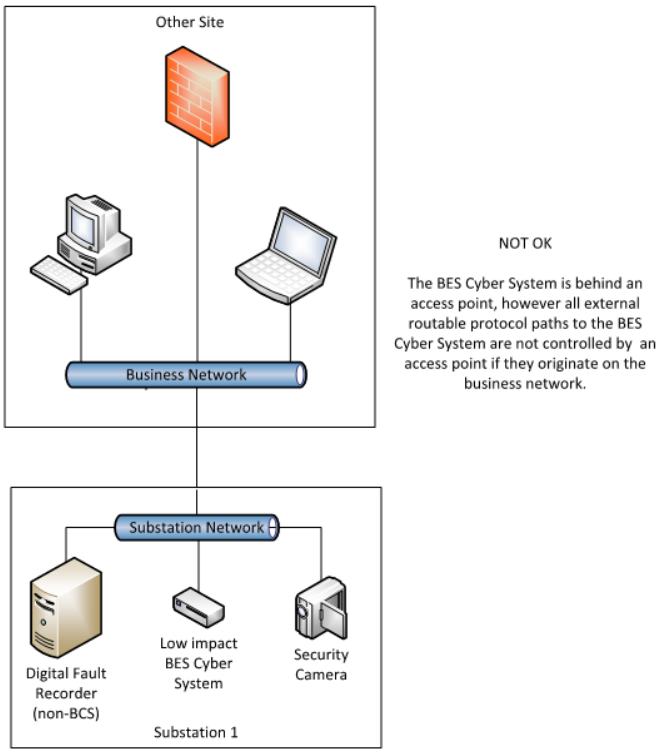
- Dialup Connectivity to a low impact BES Cyber System is set to dial out only (no autoanswer) to a preprogrammed number to deliver data. Incoming Dialup Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

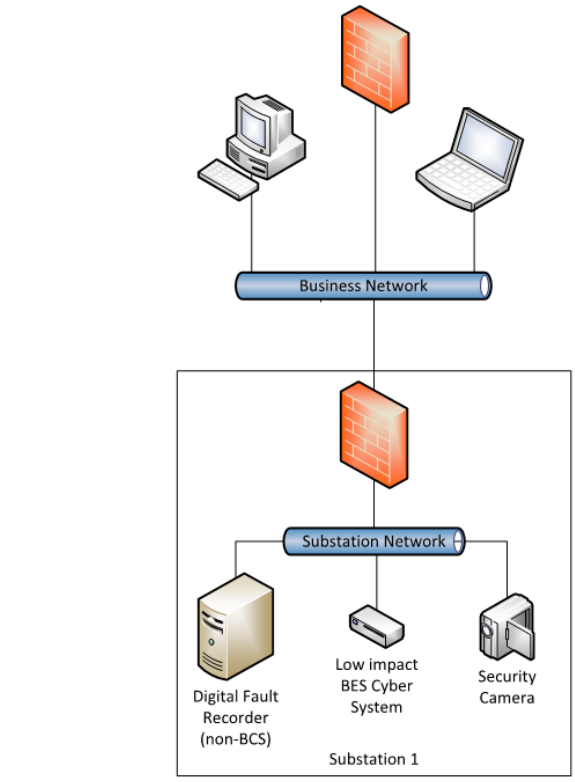
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has dialup connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset which has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

The SDT also notes that in topic 2.4, the SDT uses the term “electronic access control” in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

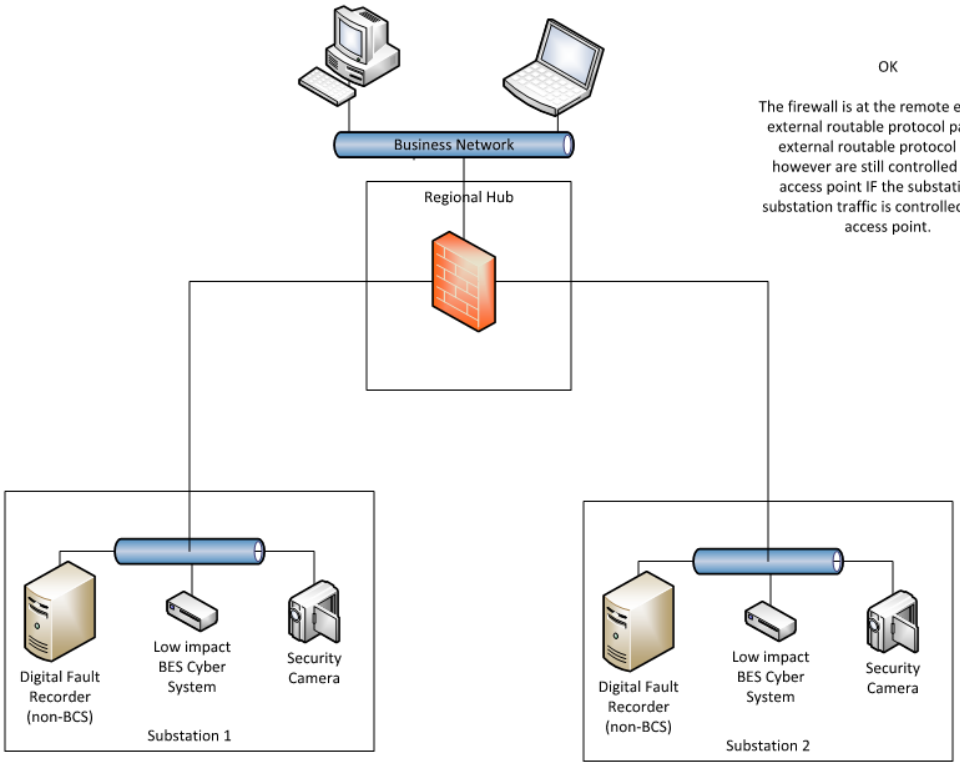
The following diagrams explain the SDT’s rationale.





OK

All the external traffic to the BES Cyber System is controlled by an access point.



OK

The firewall is at the remote end of an external routable protocol path. All external routable protocol paths however are still controlled by the access point IF the substation to substation traffic is controlled via the access point.

2.5 - The entity should have a documented cyber security incident response plan that includes each of the topics listed. For assets that have limited or no connectivity, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident. The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or paper drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

2.6 - The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel on at least a quarterly basis. The physical security, electronic access controls, and the cyber security incident response plan should be covered at least every 15 months. It is up to the entity as to the topics and how it schedules these topics. It should be sufficient for an entity to produce the awareness material that it delivered quarterly and the delivery method(s) (posters, emails, topics at staff meetings, etc.). The intent is that tracking of reception of the messages by personnel is not required.

Requirement R3:

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to

the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~5~~6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003-~~5~~ exists as part of a suite of CIP Standards related to cyber security, which ~~. CIP-002-5.1~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~ ~~**, in a manner that identifies, assesses, and corrects deficiencies, . . .**~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes,

but ~~they~~ it must address the applicable requirements. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to ~~its~~ low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements by CIP Senior Manager approval of the policies specified in Part 2.1.

The language in Requirement R2, Part 2.~~3~~ 4 "~~. . . for~~ external routable protocol ~~connections~~ paths" and "Dial-up Connectivity~~. . .~~" was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.~~3~~ 4 uses the phrase "external routable protocol ~~connections~~paths" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. The Standard Drafting Team (SDT) intent in using the phrase "external routable protocol paths" is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).

The additions to Requirement R2, in particular the processes required under Parts 2.2-2.6, address FERC Order No. 791 paragraphs 106-110, which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets. The SDT pulled language and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2.

In FERC Order No. 791 paragraphs 111-112, FERC upheld that creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.

R2. Each Responsible Entity for its assets ~~identified in CIP-002-5, Requirement R1, Part R1.3~~containing low impact BES Cyber Systems~~),~~ shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* ~~implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months:~~. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~Cyber security awareness;~~

~~Physical security controls;~~

~~Electronic access controls for external routable protocol connections and Dial-up Connectivity; and~~

~~Incident response to a Cyber Security Incident.~~

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table~~. If any asset locations have been identified per R2 of this Standard, then the following bulleted evidence may be included~~.

~~Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.~~

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
			external routable protocol paths.
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager

may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only three~~one of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only~~ two of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only one~~three of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2~~	The Responsible Entity did not ~~document or implement~~have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2, Part 2.1. (~~R2~~2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the	~~one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of	~~but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by	Part 2.1 within 18 calendar months of the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 18 calendar months of the previous approval. (~~R2~~2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R2~~2.1) OR	the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R2~~2.1)	Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~R2~~2.1) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity documented and implemented one or	The Responsible Entity did not document or implement any processes for assets with a low impact rating to include the operational or procedural control(s) to restrict physical access as required by Requirement R2, Part 2.2. (2.2) OR The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.3. (2.3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not reinforce cyber security practices at least quarterly but did reinforce cyber security practices at least every two quarters. (2.6) OR The Responsible Entity did not	OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.5. (2.5) OR	more processes for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include three of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices	The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity did not implement any Cyber Security Incident response plans for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.5 for assets with a low impact rating in less than or equal to 16 calendar months. (2.6)	The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include one of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR	at least quarterly but failed to include two of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 for assets with a low impact rating in more than 17 calendar months but less than or equal to 18 calendar months. (2.6)	implement a security awareness program for assets with a low impact rating that collectively included the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced cyber security practices at least every 15 months. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 in more than 16 calendar months but less than or equal to 17 calendar months. (2.6)		impact rating that reinforced the topics within 18 calendar months as required by Requirement R2, Part 2.6. (2.6)
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				50 calendar days of the change. (R3)		Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4)~~ ~~OR~~ ~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or~~	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~correct the deficiencies.(R4)~~ ~~OR~~ The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6~~5~~, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6~~5~~, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-6~~5~~, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not~~

~~necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.~~

The intent of the requirement is to outline a set of protections designed for all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at a programmatic or site level, not an individual device or system level.

There are four main areas that must be covered by this security program: physical security, electronic access controls for all external routable protocol paths or Dial-up Connectivity, a security awareness program, and cyber security incident response plans.

The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary.

2.1 - As with Requirement R1, the number of policies and the specific language used in them would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas in CIP-003-6, Requirement R2, Parts 2.2 through 2.6. The Responsible Entity has flexibility in the number and structure of its policies to meet its needs and organization. Examples include developing a single comprehensive cyber security policy covering these topics for all in-scope assets, several comprehensive cyber security policies based on asset type, or a single high-level umbrella policy with additional policy detail in lower level documents in its documentation hierarchy.

2.2 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.

2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been

granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity's controls.

2.4 – The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. The electronic access controls should address the risk of using the asset's external connectivity to gain access to the low impact BES Cyber Systems. The entity should be able to describe how its electronic access controls on the external connectivity paths protect the collection of low impact BES Cyber Systems at the site. The intent is to reduce the risk of aggregation of numerous low impact BES Cyber Systems at the site or across multiple sites through external connectivity.

Examples of sufficient access controls may include:

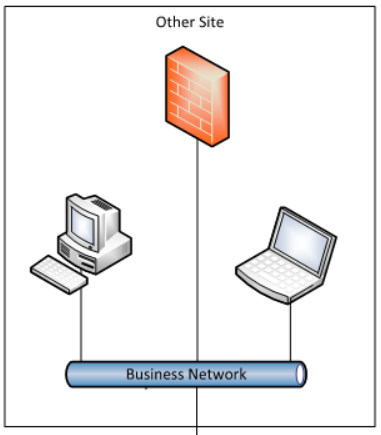
- All the external routable protocol connectivity paths to the asset pass through a firewall that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are shielded from or to the world-wide-web (e.g. IP addresses, ports, services, and data diode) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.
- Dialup Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dialup Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has dialup connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset which has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

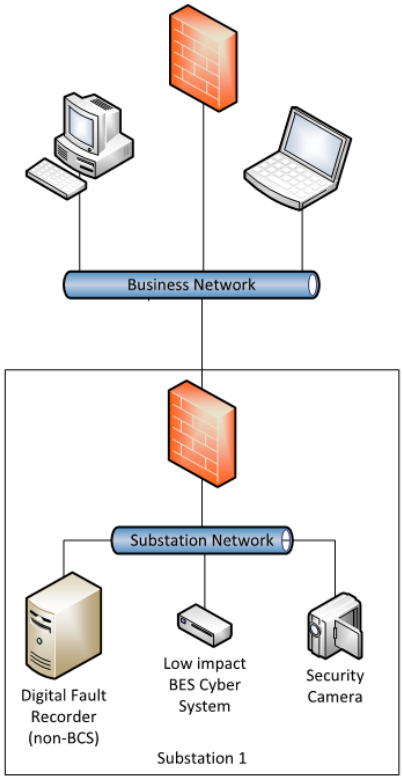
The SDT also notes that in topic 2.4, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

The following diagrams explain the SDT's rationale.



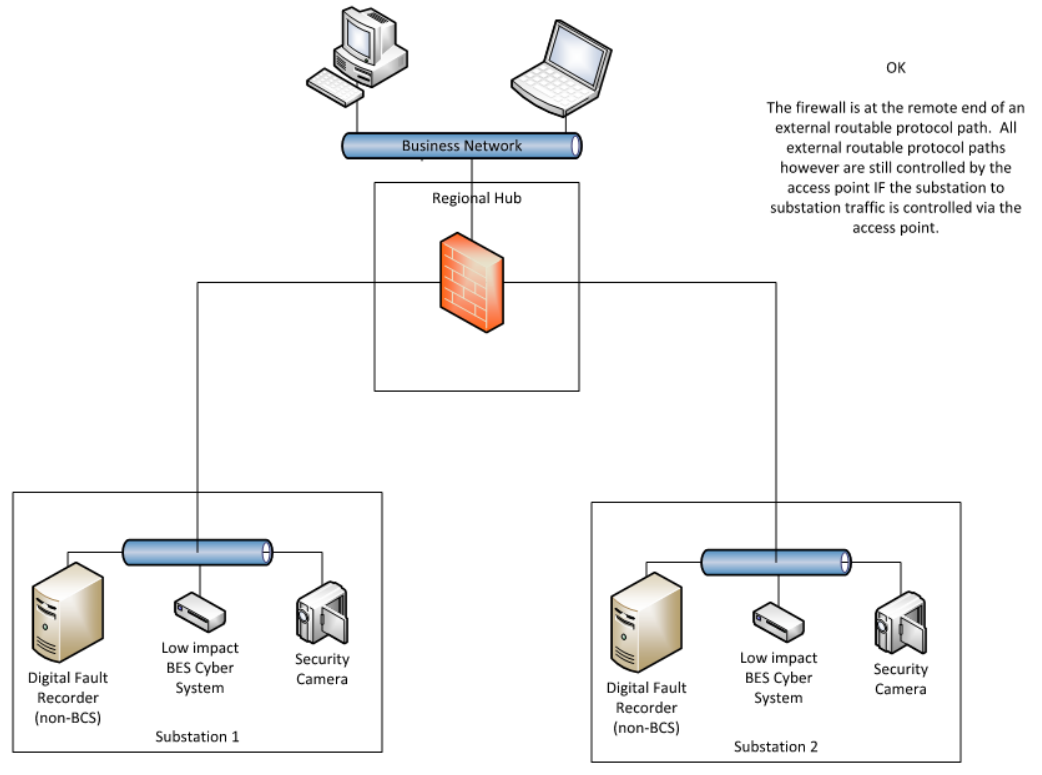
NOT OK

The BES Cyber System is behind an access point, however all external routable protocol paths to the BES Cyber System are not controlled by an access point if they originate on the business network.



OK

All the external traffic to the BES Cyber System is controlled by an access point.



2.5 - The entity should have a documented cyber security incident response plan that includes each of the topics listed. For assets that have limited or no connectivity, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident. The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or paper drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

2.6 - The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel on at least a quarterly basis. The physical security, electronic access controls, and the cyber security incident response plan should be covered at least every 15 months. It is up to the entity as to the topics and how it schedules these topics. It should be sufficient for an entity to produce the awareness material that it delivered quarterly and the delivery method(s) (posters, emails, topics at staff meetings, etc.). The intent is that tracking of reception of the messages by personnel is not required.

Requirement R3:

The intent of CIP-003-6~~5~~, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6~~5~~, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-0046 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity	did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			(3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR The Responsible Entity has implemented	individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

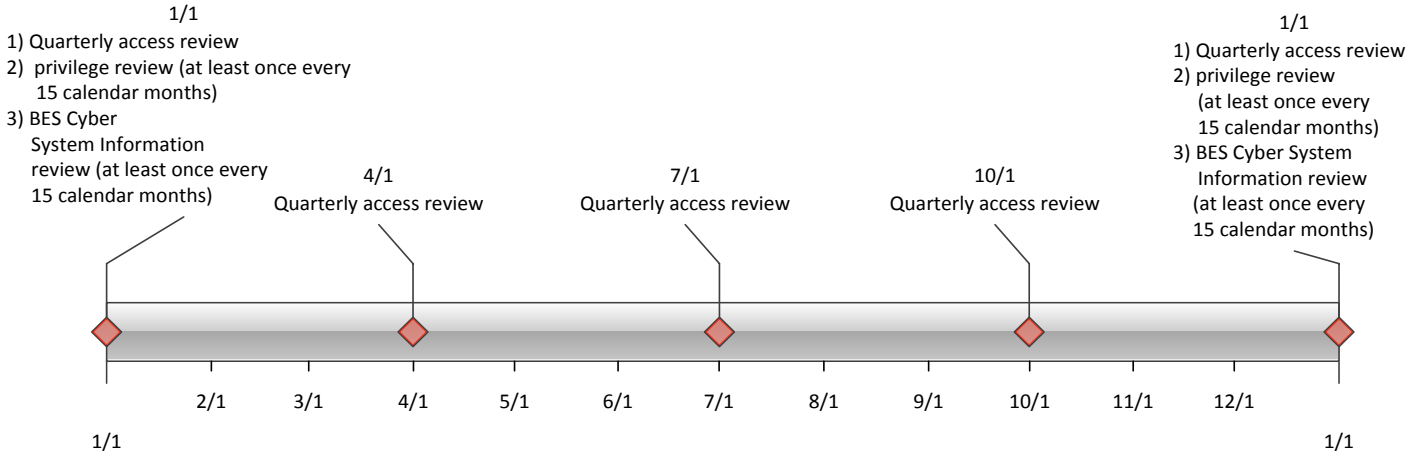
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to

or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~5.1~~6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~5.1~~6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-004 ~~5.1~~ exists as part of a suite of CIP Standards related to cyber security, which ~~CIP-002-5~~ requires the initial identification and categorization of BES Cyber Systems ~~CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards.*~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement **in a manner that identifies, assesses, and corrects deficiencies, . . .~~**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements~~

~~described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~ 6Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ ~~a~~ one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-~~5~~6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-~~5~~ 6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the~~	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the~~	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	~~deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical	~~deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	(2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date~~, and did not identify, assess and correct the deficiencies~~. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals~~, and did not identify, assess, and correct the deficiencies~~.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals~~, and did not identify, assess, and correct the deficiencies~~.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date ~~and has identified deficiencies, and did not identify, assess, and correct the deficiencies~~. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter~~, and did not identify, assess and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located~~, and did not identify, assess, and correct the deficiencies~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.4)			were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that~~-~~ an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances~~, and did not~~			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~identify, assess, and correct the deficiencies~~. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

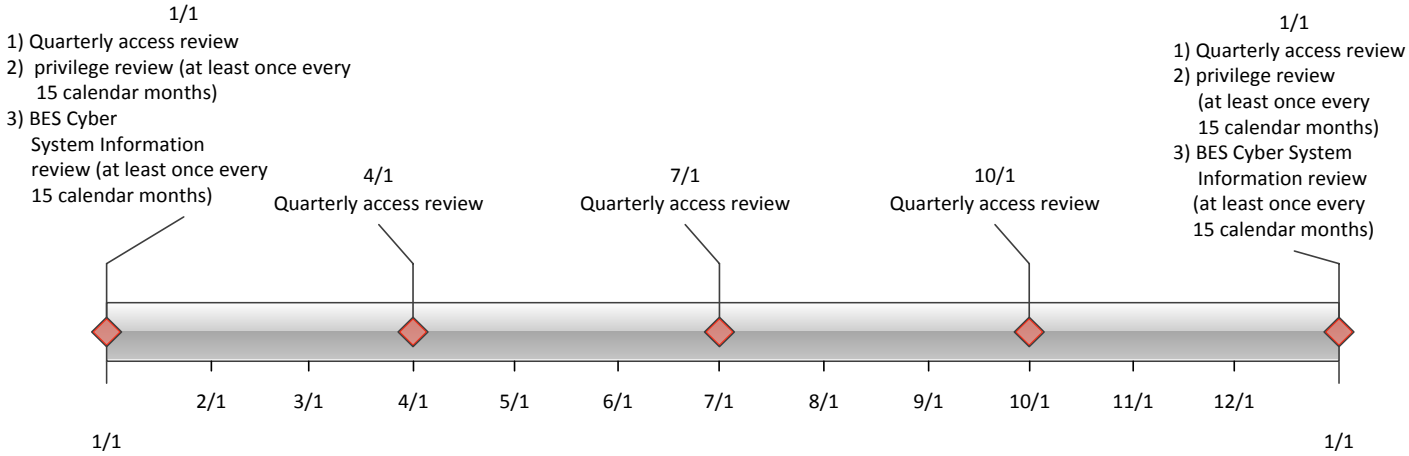
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to

or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

6. Background:

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-3 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-~~5~~6

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security, which ~~, CIP-002-5~~ requires the initial identification and categorization of BES Cyber Systems~~, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies, . . .~~**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of

300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access

authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6~~7~~ and 1.7~~8~~ beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-~~5~~6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The	N/A The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to	N/A The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar~~	~~identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)~~	~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not~~	~~documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1)~~ OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~days and identified deficiencies but did not assess or correct the deficiencies. (1.9)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)~~		~~assess or correct the deficiencies. (1.6)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)~~	~~correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2)~~ OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) ~~OR~~ ~~The Responsible Entity documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)~~ OR The Responsible Entity does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~identify, assess, or correct the deficiencies. (1.4)~~ OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical ~~security~~ Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-65)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A ~~The Responsible Entity included a visitor~~	N/A ~~The Responsible Entity included a visitor~~	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor~~	~~control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)~~	requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)~~		
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete	The Responsible Entity ~~has~~ did not document~~ed and~~ or implement~~ed~~ a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6~~7~~ and 1.7~~8~~ beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-3 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until six calendar months after the effective date of Reliability Standard CIP-007-6.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-6 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-6 Table R5*. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for

individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement but do not meet the additional obligations for transient devices.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period

called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common

configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password

guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-~~5~~6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until six calendar months after the effective date of Reliability Standard CIP-007-6.

6. Background:

Standard CIP-007 ~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5.1~~ requires the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ 2 and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on~~

~~*whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is

specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~5~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.2) ~~OR~~ ~~The Responsible Entity has~~	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.1) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for determining~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R1) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)~~	~~necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)~~	~~the deficiencies. (R1)~~
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R2 ~~and has identified deficiencies but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but~~	sources, for tracking or evaluating cyber security patches for applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or~~	applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and	~~not assess or correct the deficiencies~~. (R2)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2)~~ OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35	~~correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2)	implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for~~	security patches for applicable Cyber Assets~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but less than 50 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation~~	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct~~	~~applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4)~~OR~~ ~~The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess,~~	plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an~~	~~not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4)~~ OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4) ~~OR~~ ~~The Responsible Entity documented~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~or correct the deficiencies. (2.3)~~	~~existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)~~
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns ~~and has identified deficiencies but did~~	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code ~~and has identified deficiencies but did not assess or correct~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R3 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R3) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~not assess or correct the deficiencies~~. (3.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)~~	~~the deficiencies~~. (3.2)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used,	~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify, assess, or correct the deficiencies. (R3)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code~~ and has identified deficiencies but did not assess or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the Responsible Entity did not update malicious code protections ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (3.3)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies.~~ ~~(3.3)~~	~~the deficiencies~~. (3.1) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4) ~~The Responsible Entity has documented and~~	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.2)~~OR~~ ~~The Responsible Entity has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R4 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R4)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4~~	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2)~~ OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.1) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log events for the~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.3) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional~~	~~Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3)~~OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals~~ and has identified deficiencies but did~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (4.4)~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)~~	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for~~	process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~The Responsible Entity has implemented one or more documented process(es) for password-only~~	process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the~~	more process(es) that included the applicable items in *CIP-007-~~5~~ 6 Table R5 ~~and has identified deficiencies but did not assess or correct the deficiencies~~*. (R5) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5)~~OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2)~~OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts~~ and has identified deficiencies but did~~	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (5.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only	authentication of interactive user access~~ and did not identify, assess, or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.4) ~~OR~~ ~~The Responsible Entity has~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce	~~implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					one of the two password parameters as described in 5.5.1 and 5.5.2~~ and did not identify, assess, or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months	described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password~~	~~or correct the deficiencies. (5.5)~~ OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.7)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)~~

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for

individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, ~~portable storage media policies,~~ Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code

cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement but do not meet the additional obligations for transient devices.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible

Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of R~~r~~emovable M~~m~~edia in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor.

Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-65 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

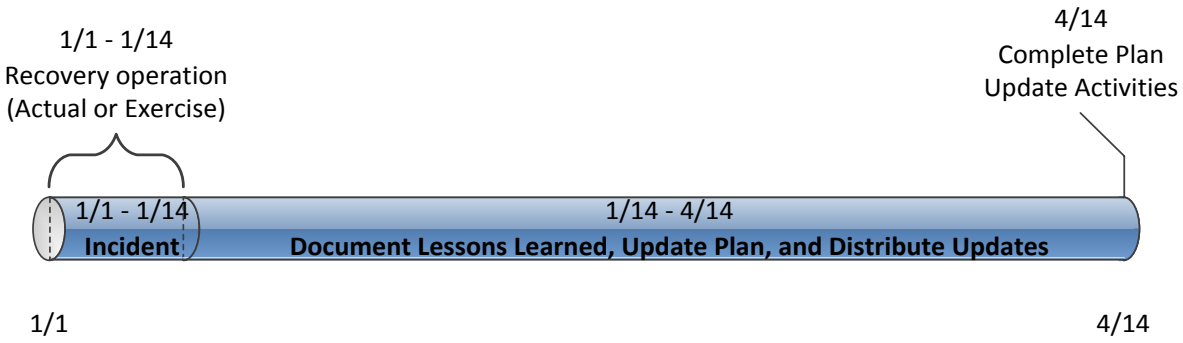


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

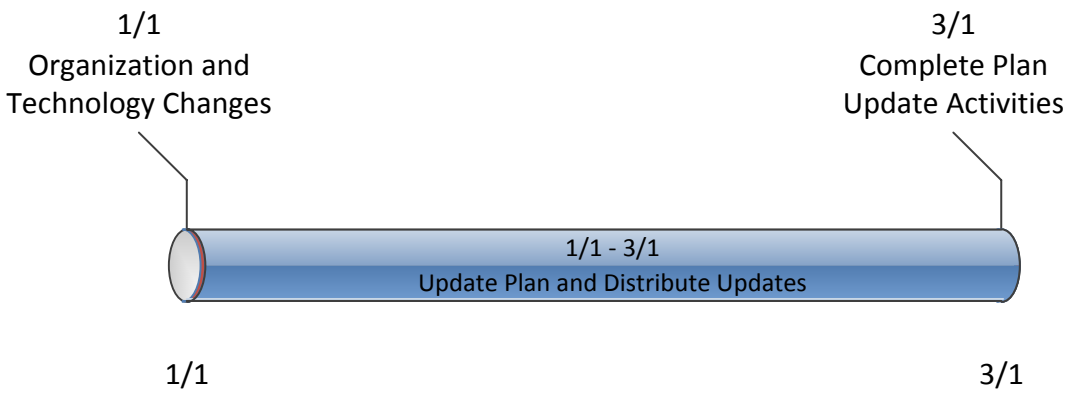


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-~~5~~6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-009 ~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which ~~. CIP-002-5.1~~ require~~s~~ the initial identification and categorization of BES Cyber Systems ~~. CIP-003-5~~6, CIP-004-56, CIP-005-5, CIP-006-56, CIP-007-56, CIP-008-5, CIP-009-56, CIP-010-12, and CIP-011-1 2 and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications*.

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	**Operations**	**Lower**	The Responsible	The Responsible	The Responsible	The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning **Real-time Operations**		Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests~~, and when tested, any~~	Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests~~, and when tested, any deficiencies were~~	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests~~, and when tested, any~~	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)~~ ~~OR~~ The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) ~~OR~~ ~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity has tested a~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)~~
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

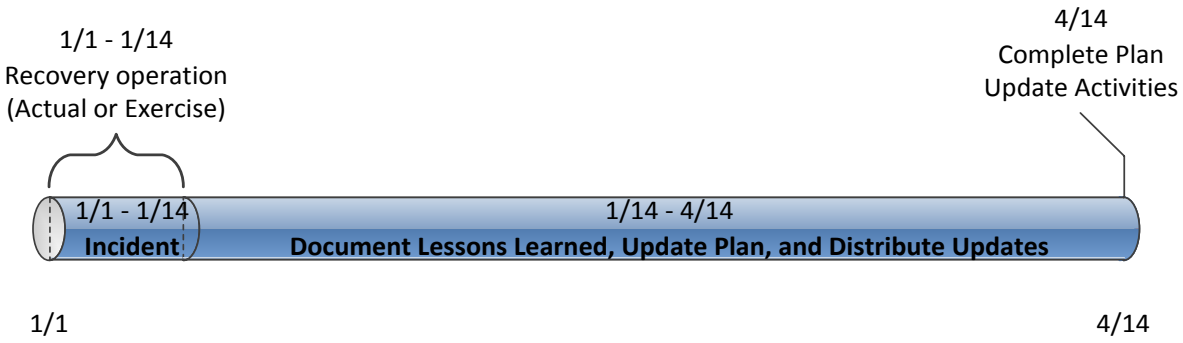


Figure 1: CIP-009-~~5~~ 6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

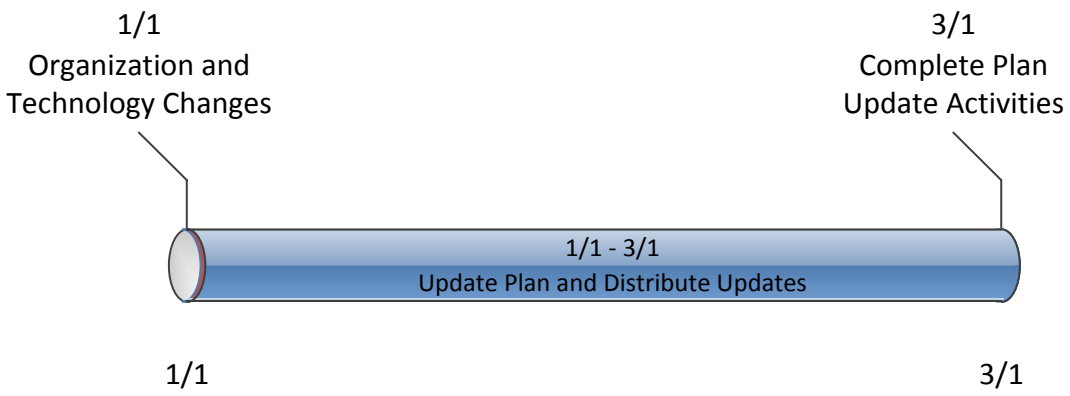


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 is to address FERC Order No. 791 Paragraphs 6 and 136, which require the standards to address security-related issues associated with tools specifically used for data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To that end, the requirement goals are as follows:

(1) Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and

(2) Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

The SDT has incorporated the concepts of other requirements from FERC-approved CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. While the requirements are similar, they are not to the same rigor of those found in CIP-007 protecting the permanent assets identified by an entity. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. Authorization shall include: 4.1.1. Users, individually or by group/role; 4.1.2. Locations, individually or by group/role; 4.1.3. Defined acceptable use; and 4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or • A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.
4.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).
4.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
4.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4. For a modification that deviates from the state in Part 4.1.4, either: • Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or • Update Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.
4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date. For security patches that are not up-to-date, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints Text

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity did not document or implement process(es) that collectively address the requirement

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of Transient Cyber Assets, but failed to include one of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include two of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include three of the required items listed in 4.1.1 through 4.1.4. (4.1) OR The Responsible Entity documented and implemented a process to evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 but did not take one of the actions required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity documented and implemented a process to evaluate	parts as required by Requirement R4. (R4) OR The Responsible Entity did not use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability) as required by Requirement R4, Part 4.2. (4.2) OR The Responsible Entity did not use method(s) to detect malicious code on Removable Media prior to use on applicable systems as required by Requirement R4, Part 4.3. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Transient Cyber Assets within 35 calendar days prior to use but did not take one of the actions required by Requirement R4, Part 4.7. (4.7)	OR The Responsible Entity did not mitigate the threat of detected malicious code for Transient Cyber Assets or Removable Media as required by Requirement R4, Part 4.4. (4.4) OR The Responsible Entity did not update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns as required by Requirement R4, Part 4.5. (4.5) OR The Responsible Entity did not evaluate Transient

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 as required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity did not evaluate Transient Cyber Assets within 35 calendar days prior to use as required by Requirement R4, Part 4.7. (4.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

This Requirement applies to any transient devices (i.e. Transient Cyber Assets and Removable Media) that will be connected temporarily to an applicable system. Examples of these devices include, but are not limited to:

- Hardware/software diagnostic test equipment
- Hardware/software packet sniffers
- Hardware/software used for BES Cyber System maintenance
- Hardware/software used for BES Cyber System configuration
- Hardware/software used to perform vulnerability assessments

Transient Cyber Assets can be in the form of a laptop, desktop, or tablet. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

This requirement does not cover hardware/software components that may support information system maintenance yet are a part of the system, for example the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of a switch.

Requirement Parts 4.1, 4.3, 4.6, and 4.7 refer to the term “prior to use” related to when specific actions must occur. For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. For example, a technician would need to have a laptop evaluated only once according to Part 4.6 when working in the same PSP. The technician would not need to have the evaluation performed each time it connects to a different Cyber Asset.

Requirement Part 4.1:

Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets. This allows entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1. User(s), individually or by group/role, allowed to use Transient Cyber Assets. This is intended to provide assurance around who has physical proximity to the Transient Cyber Assets. These user(s) must have authorized electronic and unescorted physical access to the applicable system in accordance with CIP-004.
2. Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group/role of locations. Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. It may be reasonable to have separate Transient Cyber Assets for each impact level.
3. The intended or approved use of each Transient Cyber Asset. Activities not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals on the activities or uses that are not allowed (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).
4. The operating system, firmware, and intentionally installed software. All of this information may not be available or relevant to each Transient Cyber Asset. Having this information facilitates the review in Part 4.6. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The Standard Drafting Team does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included.

CAUTION: Entities should exercise caution when using Transient Cyber Assets and ensure they do not have wireless or Bluetooth features enabled in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber

Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Requirement Parts 4.2, 4.3, 4.4, and 4.5:

Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.

It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.

For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.

For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.

Requirement Parts 4.6 and 4.7:

Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.

Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-~~1~~2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 -1 exists as part of a suite of CIP Standards related to cyber security, which. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter. The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to

~~change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 is to address FERC Order No. 791 Paragraphs 6 and 136, which require the standards to address security-related issues associated with tools specifically used for data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To that end, the requirement goals are as follows:

(1) Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and

(2) Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

The SDT has incorporated the concepts of other requirements from FERC-approved CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. While the requirements are similar, they are not to the same rigor of those found in CIP-007 protecting the permanent assets identified by an entity. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. Authorization shall include: 4.1.1. Users, individually or by group/role; 4.1.2. Locations, individually or by group/role; 4.1.3. Defined acceptable use; and 4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or • A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.
4.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).
4.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
4.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4. For a modification that deviates from the state in Part 4.1.4, either: • Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or • Update Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.
4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date. For security patches that are not up-to-date, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints Text

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified~~	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for	implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct~~	~~security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1)~~	~~changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update~~	update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~the deficiencies in the verification documentation. (1.4.3)~~		~~baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the~~	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in~~	configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencie~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~(1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~identified deficiencies but did not assess or correct the deficiencies. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)~~OR~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~not identify, assess, or correct the deficiencies. (2.1)~~
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity did not document or implement process(es) that collectively address the requirement

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of Transient Cyber Assets, but failed to include one of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include two of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include three of the required items listed in 4.1.1 through 4.1.4. (4.1) OR The Responsible Entity documented and implemented a process to evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 but did not take one of the actions required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity documented and implemented a process to evaluate	parts as required by Requirement R4. (R4) OR The Responsible Entity did not use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability) as required by Requirement R4, Part 4.2. (4.2) OR The Responsible Entity did not use method(s) to detect malicious code on Removable Media prior to use on applicable systems as required by Requirement R4, Part 4.3. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Transient Cyber Assets within 35 calendar days prior to use but did not take one of the actions required by Requirement R4, Part 4.7. (4.7)	OR The Responsible Entity did not mitigate the threat of detected malicious code for Transient Cyber Assets or Removable Media as required by Requirement R4, Part 4.4. (4.4) OR The Responsible Entity did not update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns as required by Requirement R4, Part 4.5. (4.5) OR The Responsible Entity did not evaluate Transient

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 as required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity did not evaluate Transient Cyber Assets within 35 calendar days prior to use as required by Requirement R4, Part 4.7. (4.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-~~5~~6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-~~5~~ 6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

This Requirement applies to any transient devices (i.e. Transient Cyber Assets and Removable Media) that will be connected temporarily to an applicable system. Examples of these devices include, but are not limited to:

- Hardware/software diagnostic test equipment
- Hardware/software packet sniffers
- Hardware/software used for BES Cyber System maintenance
- Hardware/software used for BES Cyber System configuration
- Hardware/software used to perform vulnerability assessments

Transient Cyber Assets can be in the form of a laptop, desktop, or tablet. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

This requirement does not cover hardware/software components that may support information system maintenance yet are a part of the system, for example the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of a switch.

Requirement Parts 4.1, 4.3, 4.6, and 4.7 refer to the term “prior to use” related to when specific actions must occur. For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. For example, a technician would need to have a laptop evaluated only once according to Part 4.6 when working in the same PSP. The technician would not need to have the evaluation performed each time it connects to a different Cyber Asset.

Requirement Part 4.1:

Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets. This allows entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1. User(s), individually or by group/role, allowed to use Transient Cyber Assets. This is intended to provide assurance around who has physical proximity to the Transient Cyber Assets. These user(s) must have authorized electronic and unescorted physical access to the applicable system in accordance with CIP-004.
2. Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group/role of locations. Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. It may be reasonable to have separate Transient Cyber Assets for each impact level.
3. The intended or approved use of each Transient Cyber Asset. Activities not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals on the activities or uses that are not allowed (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).
4. The operating system, firmware, and intentionally installed software. All of this information may not be available or relevant to each Transient Cyber Asset. Having this information facilitates the review in Part 4.6. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The Standard Drafting Team does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included.

CAUTION: Entities should exercise caution when using Transient Cyber Assets and ensure they do not have wireless or Bluetooth features enabled in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber

Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Requirement Parts 4.2, 4.3, 4.4, and 4.5:

Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.

It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.

For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.

For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.

Requirement Parts 4.6 and 4.7:

Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.

Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~1~~2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-011 ~~-1~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it~~-~~ believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~1~~ 2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~1~~ 2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~1~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify,~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~assess, or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~but did not identify, assess, or correct the deficiencies. (1.2)~~	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. A Transient Cyber Asset is not a BES Cyber Asset.

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset.

Removable Media: Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.

Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. ~~(~~A Transient Cyber Asset is not a BES Cyber Asset. ~~if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)~~

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset. ~~if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.~~

Removable Media: Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.

Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

June 2, 2014

Requested Approvals

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel and Training
- CIP-006-6 — Cyber Security — Physical Security
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009–6 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-2 — Cyber Security — Configuration Change Management
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5 — Cyber Security — Personnel and Training
- CIP-006-5 — Cyber Security — Physical Security
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. A Transient Cyber Asset is not a BES Cyber Asset.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset.

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.
Transient Cyber Asset	A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date that entities must begin to comply that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-6 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-003-6, Requirement R2

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

2. CIP-004-6 — Cyber Security — Personnel and Training

   Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-006-6, Requirement R1, Part 1.10

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-6 —Cyber Security — Systems Security Management

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until six calendar months after the effective date of Reliability Standard CIP-007-6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems

   Reliability Standard CIP–009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-2 — Cyber Security — Configuration Change Management

   Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-010-2, Requirement R4

   Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

7. CIP-011-2 — Cyber Security — Information Protection

   Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

   The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

9. Standards for Retirement

   Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[1] (Version 5 Plan) remain the same:

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

[1] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2014-02 CIP Version 5 Revisions – Cyber Security Standards

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the proposed draft CIP standards. The electronic comment form must be completed by **8 p.m. Eastern, July 16, 2014**.

All documents and information about this project are available on the project page. If you have questions please contact Marisa Hecht at marisa.hecht@nerc.net or by telephone at 404-446-9620 or Ryan Stewart at ryan.stewart@nerc.net or by telephone at 202-644-8091.

Background Information

On November 22, 2013, FERC issued Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*. In this order, FERC approved version 5 of the CIP standards, and also directed that NERC make the following modifications to those standards:

1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for Low Impact assets.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the "identify, assess, and correct" language and communication networks by February 3, 2015, one year from the effective date of FERC Order No. 791. FERC did not place any time frame for NERC to respond to the Low Impact and transient electronic devices directives.

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

Questions

1. The Standard Drafting Team (SDT) developed objective criteria in the processes in CIP-003, Requirement R2 to address the directive in FERC Order No. 791. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

2. The SDT developed CIP-006, Requirement R1, Part 1.10 and revised CIP-007, Requirement R1, Part 1.2 to meet the directive in FERC Order No. 791 to address protections for nonprogrammable components of communication networks. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

3. The SDT developed CIP-010, Requirement R4 and revised CIP-004, Requirement R1, Part 2.1.9 to meet the directive in FERC Order No. 791 to address transient devices (Transient Cyber Assets and Removable Media). Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

4. The SDT proposed new definitions for Transient Cyber Assets and Removable Media and revised definitions for BES Cyber Asset and Protected Cyber Assets. Do you agree with the new and revised definition? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

5. The SDT removed the Identify, Assess, and Correct (IAC) language from 17 requirements to meet the directive in FERC Order No. 791 to remove or modify the IAC language. Do you support this revision approach? If not, why not and what alternative approach do you recommend?

   Yes:

   No:

   Comments:

6. The Implementation Plan uses the existing effective date of the FERC approved CIP V5 Standards for CIP-003-6 Requirement R2 and provides additional time for compliance for CIP-006-6, Requirement R1, Part 1.10; CIP-007-6, Requirement R1, Part 1.2; and CIP-010-2, Requirement R4. Are the timeframes reasonable and appropriate? If not, please explain.

   Yes:

   No:

   Comments:

7. Are there any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

   Yes:

   No:

   Comments:

8. Do you have input on other areas, within the scope of the Standards Authorization Request, for the standards or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions.

   Yes:

   No:

   Comments:

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791
June 2, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
106	Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact	The SDT revised Requirement R2 of CIP-003-6 to include additional specificity regarding the processes that responsible entities must have for low impact facilities. In addition, the SDT developed objective criteria surrounding the controls for

[2] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 186, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.	some entities based on asset-type and routability. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category. The SDT confined these revisions in CIP-003-6, Requirement R2 to the following four technical areas: 1. **Physical Security Controls:** Parts 2.2 and 2.3 and their subparts require controls to restrict physical access to Low Impact BES Cyber Systems and require additional protections for Controls Centers. 2. **Electronic Access Controls:** Part 2.4 and its subparts address protections around external routable protocol paths and Dial-up Connectivity. 3. **Cyber Security Incident Response:** Part 2.5 and its subparts outline the criteria required to be in a Cyber Security Incident response plan. 4. **Cyber Security Awareness:** Part 2.6 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices and Parts 2.2 through 2.5 of Requirement R2. The SDT determined that adding

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		intervals increases the auditability of the requirement part. In addition to the revisions to the four technical areas, the SDT retained the requirement in Part 2.1 to obtain CIP Senior Manager approval of one or more documented policies that address the topics in Parts 2.2 – 2.6.
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail	NERC proposes to conduct a survey of Cyber Assets, pursuant to Section 1600 of the NERC *Rules of Procedure* (ROP), regarding the scope of the term "BES Cyber Asset." In accordance with Section 1600 of the ROP, NERC may request data or information from Registered Entities that is necessary to meet NERC's obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of FERC's regulations. The purpose of the proposed Data Request is to respond to FERC's directive from Order No. 791 to conduct a survey regarding the scope of the term "BES Cyber Asset" and submit an informational filing based on the data collected by February 3, 2015.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	
132	Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.	The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which includes a set of controls to provide higher assurance against the propagation of malware prior to connecting transient devices. The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition. The drafting team determined entities manage these transient devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The Commission provides a list of security controls it expects NERC to consider for addressing transient devices, and the consideration of each security element is described as follows: 1. **Device authorization as it relates to users and locations:** CIP-010-2 Requirement R4, Part 4.1 requires entities to authorize Transient Cyber Assets and Removable Media by individual(s) and location(s) prior to connecting them to the BES Cyber System. **2. Software authorization:** CIP-010-2 Requirement R4, Part 4.1 borrows similar language from CIP-010-2 Requirement R4, Part 1.1 to authorize intentionally installed software on Transient Cyber Assets. **3. Security patch management:** CIP-010-2 Requirement R4, Part 4.7 requires entities to install patches on Transient Cyber Assets and Removable Media, at least once every 35 calendar days, or prior to use, in connecting to the BES Cyber System. 4. **Malware prevention:** CIP-010-2 Requirement R4, Part 4.2 requires entities to have malware protection on the Transient Cyber Asset. Requirement R4, Part 4.3 requires malware protection for Removable Media prior to connection, and Requirement R4, Part 4.5 requires up-to-date malware signatures. 5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		control and determined the Reliability Standards already address the vulnerabilities this control attempts to mitigate, and additional guidance is necessary in CIP-011-2 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient devices. Specifically, the drafting team determined the two primary objectives in controlling physical access to transient devices are (1) preventing the introduction of malware and (2) preventing the unauthorized release of BES Cyber System Information. The latter objective is sufficiently addressed with the requirements in CIP-011-2 to protect and securely handle BES Cyber System Information. The objective to prevent the introduction of malware is sufficiently addressed through the malware protection requirement proposed for transient devices. Ensuring the physical protection of transient devices outside of the PSP is in some cases more burdensome to the entity than receiving the full protection of the Standard, and has minimal effect to prevent the introduction of malware. 6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-2 requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-2 Requirement R4.
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to the CIP version 5 Standards.4 The Commission agrees that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from	NERC modified the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[3] *See infra* P 223.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	NERC modified the VRF assignment for CIP-004-5.1, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-6,

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-5, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language. 2. **VSLs for CIP-004-5.1, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-5, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the timeframe contained in the VSLs from 90-210 days to 90-120 days.

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 (CIP-002-5, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-6 R1	No change.
CIP-003-5 R1.1	CIP-003-6 R1.1	No change.
CIP-003-5 R1.2	CIP-003-6 R1.2	No change.
CIP-003-5 R1.3	CIP-003-6 R1.3	No change.
CIP-003-5 R1.4	CIP-003-6 R1.4	No change.
CIP-003-5 R1.5	CIP-003-6 R1.5	No change.
CIP-003-5 R1.6	CIP-003-6 R1.6	No change.
CIP-003-5 R1.7	CIP-003-6 R1.7	No change.
CIP-003-5 R1.8	CIP-003-6 R1.8	No change.
CIP-003-5 R1.9	CIP-003-6 R1.9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2	CIP-003-6 R2, CIP-003-6, R2.1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. The main requirement was modified to follow a similar structure to parent Requirements of those requirement parts in the table format. The CIP Senior Manager review and approval at least once every 15 months was mapped to CIP-003-6 R2.1.
CIP-003-5 R2.1	CIP-003-6 R2.6	The security awareness requirement part was mapped to Part 2.6 to reinforce cyber security practices at least quarterly, while addressing Parts 2.2 through 2.5 once every 15 calendar months. This added objective criteria to security awareness, while not to the rigor of Medium and High BES Cyber Systems.
CIP-003-5 R2.2	CIP-003-6 R2.2	Expanding the physical security controls, Part 2.2 addresses operational or procedural control(s) to restrict physical access.
NEW	CIP-003-6 R2.3	Expanding the physical security controls, Part 2.3 requires implementation of processes to include Parts 2.3.1 and 2.3.2 for low impact BES Cyber Systems at Control Centers.
NEW	CIP-003-6 R2.3.1	Expanding the physical security controls, Part 2.3.1 addresses escorted access of visitors at Control Centers.
NEW	CIP-003-6 R2.3.2	Expanding the physical security controls, Part 2.3.2 addresses monitored physical access point(s) at Control Centers with external routable protocol paths.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.3	CIP-003-6 R2.4	The electronic access controls were added as Part 2.4. The documented process(es) collectively must include Parts 2.4.1 through 2.4.3.
NEW	CIP-003-6 R2.4.1	Expanding the electronic access controls, Part 2.4.1 addresses all external routable protocol paths, if any, as needing to be through one or more identified access point(s).
NEW	CIP-003-6 R2.4.2	Expanding the electronic access controls, Part 2.4.2 addresses requiring inbound and outbound access permissions for each identified access point, including the reason for granting access, and deny all other access by default.
NEW	CIP-003-6 R2.4.3	Expanding the electronic access controls, Part 2.4.3 addresses authentication when establishing Dial-Up Connectivity, per Cyber Asset capability.
CIP-003-5 R2.4	CIP-003-6 R2.5	The incident response to a Cyber Security Incident requirement part remains in Part 2.5. The documented response plan(s) collectively must include Parts 2.5.1 through 2.5.6.
NEW	CIP-003-6 R2.5.1	Expanding the incident response controls, Part 2.5.1 address the identification, classification, and response to Cyber Security Incidents.
NEW	CIP-003-6 R2.5.2	Expanding the incident response controls, Part 2.5.2 addresses whether an identified Cyber Security Incident is reportable.
NEW	CIP-003-6 R2.5.3	Expanding the incident response controls, Part 2.5.3 addresses the notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-003-6 R2.5.4	Expanding the incident response controls, Part 2.5.4 addresses the roles and responsibilities of Cyber Security Incident response groups or individuals.
NEW	CIP-003-6 R2.5.5	Expanding the incident response controls, Part 2.5.5 addresses the incident handling procedures for Cyber Security Incidents.
NEW	CIP-003-6 R2.5.6	Expanding the incident response controls, Part 2.5.6 addresses the testing of the plan(s) at least once per 36 calendar months.
CIP-003-5 R3	CIP-003-6 R3	No change.
CIP-003-5 R4	CIP-003-6 R4	To respond to the FERC Order 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-6 R1	No change.
CIP-004-5.1 R1.1	CIP-004-6 R1.1	No change.
CIP-004-5.1 R2	CIP-004-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken. The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement “a cyber security training program(s).” That modification was made for clarity and consistency across the standards.
CIP-004-5.1 R2.1	CIP-004-6 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-6 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-6 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-6 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-6 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-6 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-6 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-6 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-6 R2.1.8	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.1.9	CIP-004-6 R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity's cyber security training program. The training must address cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.
CIP-004-5.1 R2.2	CIP-004-6 R2.2	No change.
CIP-004-5.1 R2.3	CIP-004-6 R2.3	No change.
CIP-004-5.1 R3	CIP-004-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-004-5.1 R3.1	CIP-004-6 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-6 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-6 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-6 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-6 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-6 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-6 R3.5	No change.
CIP-004-5.1 R4	CIP-004-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-004-5.1 R4.1	CIP-004-6 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-6 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-6 R4.1.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R4.1.3	CIP-004-6 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-6 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-6 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-6 R4.4	No change.
CIP-004-5.1 R5	CIP-004-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R5.1	CIP-004-6 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-6 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-6 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-6 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-6 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-6 R1.1	No change.
CIP-007-5 R1.2	CIP-007-6 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-6 R2.1	No change.
CIP-007-5 R2.2	CIP-007-6 R2.2	No change.
CIP-007-5 R2.3	CIP-007-6 R2.3	No change.
CIP-007-5 R2.4	CIP-007-6 R2.4	No change.
CIP-007-5 R3	CIP-007-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R3.1	CIP-007-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.2	CIP-007-6 R3.2	No change.
CIP-007-5 R3.3	CIP-007-6 R3.3	No change.
CIP-007-5 R4	CIP-007-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R4.1	CIP-007-6 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-6 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-6 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-6 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-6 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-6 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-6 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-6 R4.3	No change.
CIP-007-5 R4.4	CIP-007-6 R4.4	No change.
CIP-007-5 R5	CIP-007-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R4	CIP-007-6 R4	No change.
CIP-007-5 R5	CIP-007-6 R5	No change.
CIP-007-5 R5.1	CIP-007-6 R5.1	No change.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.4	CIP-007-6 R5.4	No change.
CIP-007-5 R5.5	CIP-007-6 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-6 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-6 R5.5.2	No change.
CIP-007-5 R6	CIP-007-6 R6	No change.
CIP-007-5 R7	CIP-007-6 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-2 R1.1	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-2 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-2 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-2 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-2 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-2 R1.5.2	No change.
CIP-010-1 R2	CIP-010-2 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-2 R2.1	No change.
CIP-010-1 R3	CIP-010-2 R3	No change.
CIP-010-1 R3.1	CIP-010-2 R3.1	No change.
CIP-010-1 R3.2	CIP-010-2 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-2 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-2 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-2 R3.3	No change.
CIP-010-1 R3.4	CIP-010-2 R3.4	No change.
NEW	CIP-010-2 R4	To respond to the FERC Order No. 791 directive to address transient devices, new Requirement R4 follows the table format to ensure Registered Entities implemented one or more documented process(es) that collectively include each of the applicable parts in CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection. All of the new Requirement Parts under Requirement R4 are in response to this directive.
NEW	CIP-010-2 R4.1	Part 4.1 ensures Responsible Entities authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. The authorization shall include the Requirement Parts 4.1.1 through 4.1.4.
NEW	CIP-010-2 R4.1.1	Authorization shall include users, individually or by group/role.
NEW	CIP-010-2 R4.1.2	Authorization shall include locations, individually or by group/role.
NEW	CIP-010-2 R4.1.3	Authorization shall include defined acceptable use.
NEW	CIP-010-2 R4.1.4	Authorization shall include operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-2 R4.2	Part 4.2 ensures Responsible Entities use method(s) to deter, detect, or prevent malicious code introduction on Transient Cyber Assets (per Cyber Asset capability).
	CIP-010-2 R4.3	Part 4.3 ensures Responsible Entities use method(s) to detect malicious code on Removable Media prior to use on applicable systems.
NEW	CIP-010-2 R4.4	Part 4.4 ensures Responsible Entities mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.
NEW	CIP-010-2 R4.5	Part 4.5 ensures Responsible Entities update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.
NEW	CIP-010-2 R4.6	Part 4.6 ensures Responsible Entities evaluate Transient Cyber Assets prior to use for modifications that deviate from Part 4.1.4.
NEW	CIP-010-2 R4.7	Part 4.7 ensures Responsible Entities evaluate Transient Cyber Assets periodically to ensure security patches are up-to-date.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-2 R1.1	No change.
CIP-011-1 R1.2	CIP-011-2 R1.2	No change.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R2	CIP-011-2 R2	No change.
CIP-011-1 R2.1	CIP-011-2 R2.1	No change.
CIP-011-1 R2.2	CIP-011-2 R2.2	No change.

Frequently Asked Questions

'Identify, Assess, Correct' (IAC) and the Reliability Assurance Initiative (RAI)

1. What was the intent of IAC?

The IAC concept acknowledged that for certain CIP requirements, in a changing risk landscape, engaging entities as partners to identify and correct their own reliability issues has a positive impact on Bulk Electric System reliability.

The intent of IAC was to encourage and reward entities for establishing practices (e.g. internal controls) to effectively manage implementation of high frequency security obligations.

The IAC language obligated entities to establish processes to identify less than 100% performance of reliability standards, assess the impact of this performance gap, and implement corrective action that would ultimately improve Bulk Electric System reliability.

IAC intended to shift the emphasis of compliance monitoring and enforcement activities away from the incidents of deficiency and to focus instead on identifying areas of risk along with effective governance and business practices and implementing corrective action to ensure Bulk Electric System reliability.

2. What are the Order 791 and Industry Concerns with IAC?

From FERC Order 791, the following citations illustrate the concerns:

- Paragraph 4: "…overly-vague, lacking basic definition and guidance that is needed, for example, to distinguish a successful internal control program from one that is inadequate…"
- Paragraph 35: "…is unclear with respect to the implementation and compliance obligations that language imposes and that it is too vague to audit and enforce…"
- Paragraph 46: "…NERC has not explained what is expected of responsible entities or the intended meaning of the individual terms "identify," "assess," "correct," and "deficiencies" as they are used…"
- Paragraph 48: "…does not identify a reasonable timeframe for identifying, assessing and correcting deficiencies…"
- Paragraph 49: "…does not explain whether a responsible entity is required to disclose the identified deficiencies…"
- Paragraph 75: "…we believe that a more appropriate balance might be struck to address the underlying concerns by developing compliance and enforcement processes that would grant NERC and the Regional Entities the ability to decline to pursue low risk violations of the Reliability Standards."

3. How do the RAI program concepts relate to IAC?

RAI seeks to scale compliance monitoring activities based on risk, as well as provide an alternative to enforcement proceedings for instances of non-compliance that pose lesser risk to the BES.

Like IAC, RAI seeks to encourage entities to establish and monitor effective practices (e.g. internal controls) that promote bulk electric system reliability.

RAI seeks to apply the IAC intent at the compliance and enforcement level rather than within the Standards and goes beyond CIP by applying to the broader set of NERC Reliability Standards.

RAI shifts the paradigm from pursuing every incidence of non-compliance to identifying areas of bulk electric system risk, assessing the impact of this risk, and mitigating the root cause of risk elements.

In Order 791, FERC acknowledges in Paragraph 4: "We support NERC's move away from a "zero tolerance" approach to compliance, the development of strong internal controls by responsible entities, and NERC's development of standards that focus on the activities that have the greatest impact on Bulk-Power System reliability."

4. How has the SDT chosen to address the concerns of IAC?

The SDT discussed the concerns and options within FERC Order 791 and revised the 17 requirements containing IAC by removing the language. The approach fulfils the Order 791 directive regarding the IAC language and leaves resolution of "zero defect" or "zero tolerance" to the RAI 'discretionary path to enforcement' implementation.

5. Will RAI replace the programmatic approach contemplated under IAC?

Yes. The new processes in compliance monitoring and enforcement created through RAI will allow NERC and the Regional Entities to acknowledge the types of practices that were envisioned under IAC and to determine whether any specific noncompliance should be processed as a violation.

6. How will RAI apply to the CIP Requirements that used to contain IAC?

Under the RAI enforcement approach, NERC and the Regional Entities will evaluate an entity's overall risk to reliability and the bulk power system (e.g. registered functions, internal controls and past compliance performance) and establish a compliance monitoring and enforcement treatment commensurate with the entity's risk profile and the risk posed by any instances of noncompliance.

In determining the appropriate resolution of noncompliance, NERC and Regional Entities will take into account those practices (e.g. internal controls) that contribute to the overall reduction of risk associated with possible violations.

The RAI approach should reduce the administrative burden associated with high frequency, low risk violations by allowing qualified entities to log minimal risk noncompliance and by disposing of minimal risk noncompliance through streamlined means; including NERC and Regional Entities potentially declining to pursue such issues through enforcement.

7. What are the CIP compliance obligations under RAI? Will RAI reduce the compliance obligation of the CIP standards? How will CIP audits change? Overall, does the removal of IAC change an entity's compliance obligations?

RAI will not replace, modify or reduce the compliance obligation for reliability standards. RAI processes will help address how any areas of noncompliance will be assessed and resolved. The removal of IAC will modify compliance obligations because the standards language will change and Registered Entities will no longer have to incorporate IAC into their compliance programs.

8. What is expected of Entities in maintaining records of deficiencies?

Under RAI, entities that qualify for the logging program will maintain a log of minimal risk noncompliance to be submitted to Regional Entities on a periodic basis.

9. What is a compliance exception? How do entities qualify for compliance exception?

A compliance exception is a matter that is not to be pursued through enforcement. It represents the exercise of enforcement discretion. At this point, to qualify for enforcement discretion, the noncompliance must have posed a minimal risk to the reliability of the Bulk Electric System. Noncompliance may be recorded as a compliance exception regardless of the discovery methodology (e.g. self-assessment, audit, etc.).

10. Can entities choose to participate in RAI or to retain the traditional audit/enforcement approach? If an entity chooses to not participate in RAI, what are their alternate approaches to address the IAC concerns?

Registered Entities may choose to participate by sharing information about their internal controls demonstrating that they have policies and procedures in place to ensure compliance with NERC Reliability Standards and Bulk Electric System reliability. Consequently, Regional

Entities may be able to obtain reasonable assurance of compliance with alternative compliance monitoring engagements.

In the absence of internal controls, the Regional Entities will utilize other available information to assess Registered Entity Risk and appropriate compliance monitoring scope. Regional Entities will be utilizing other RAI techniques to assess regional risk to the Bulk Electric System. Regional Entities will perform inherent risk assessments on Registered Entities to determine how regionally identified risk may or may not affect particular entities.

Compliance monitoring scope will be based upon this inherent risk assessment, assuming that no internal controls are in place at the Registered Entity that would reduce regional reliability risk. An entity that chooses not to share information regarding internal controls or participate in the evaluation process will not be able to participate in all RAI programs (e.g. the logging program). However, enforcement discretion is available to NERC and the Regional Entities with respect to minimal risk noncompliance regardless of the result of the evaluation of internal controls of a particular registered entity.

11. Explain the roles of NERC and the Regional Entities in compliance and enforcement under RAI. Will there be Regional consistency or at least coherence across regional programs?

The enforcement processes created under RAI were developed jointly by NERC and the Regional Entities. The risk associated with a specific instance of noncompliance is the main factor in determining the disposition of the issue. The most comprehensive discussion of how risk of noncompliance is assessed by NERC and the Regional Entities is found in the Self-Report User Guide, developed jointly by NERC and the Regional Entities.

12. Is a risk assessment required for entities whether they choose to participate in the RAI program or not?

The RAI program includes a risk assessment of each registered entity to determine the following aspects:

- Assessing Reliability Risks - Every registered entity has inherent risk and control risks. The ERO Enterprise must take these risks into account when monitoring compliance to establish reasonable assurance of compliance to the reliability standards. Each registered entity can voluntarily elect to work with the appropriate Regional Entity to assess and prioritize its risks, or it can voluntarily elect not to participate.
- Scoping Compliance Monitoring - The ERO Enterprise will scope the compliance monitoring for each registered entity in accordance with results of the entity's risk assessment. An entity can voluntarily establish internal controls designed to reduce its control risk which

could have a positive influence on the scoping of compliance monitoring by the Regional Entity. Conversely, the entity can voluntarily elect not to establish internal controls or share them with the Regional Entity, which would also affect how the Regional Entity scopes monitoring for that particular entity.

- Internal Controls Evaluation - An assessment of an entity's internal controls is necessary in order for an entity to participate in the aggregation/logging program. Once a common ERO enterprise methodology for such assessment is defined, that will constitute the assessment process. Entities currently being added to the program have been assessed by the Regional Entity through the Regional Entity's existing methodology.

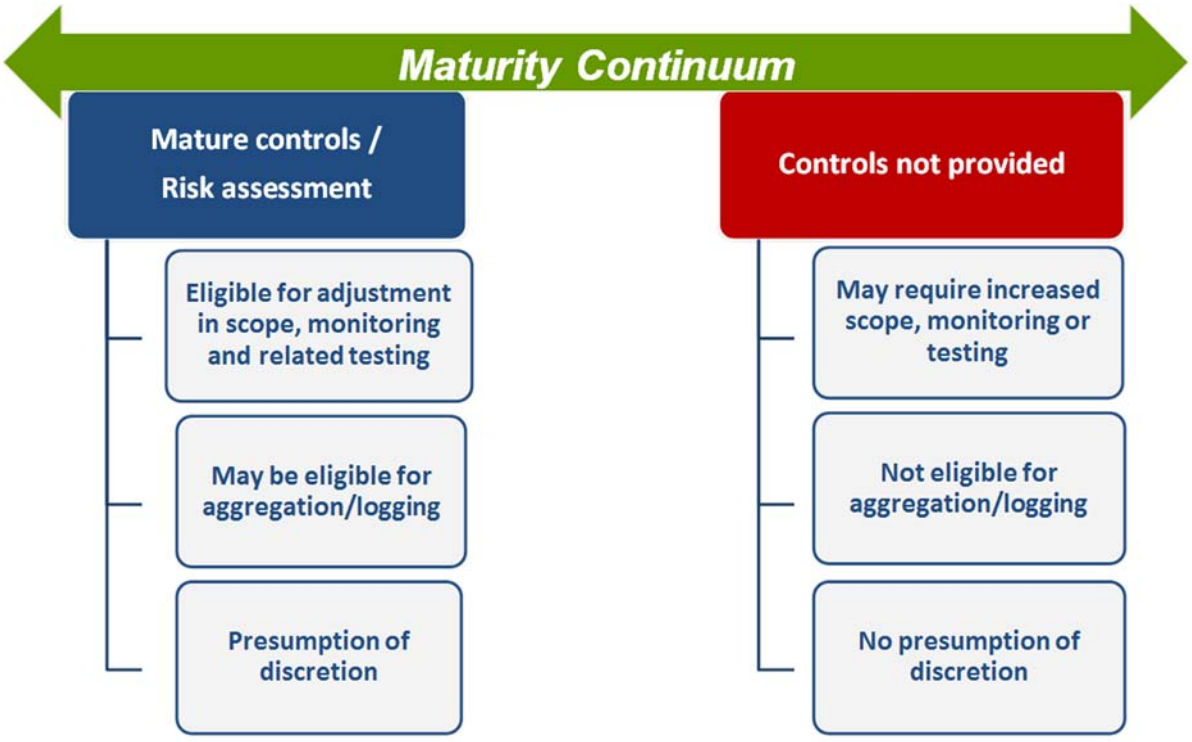
13. What is enforcement discretion? How do entities qualify for enforcement discretion? Does an entity need to apply for enforcement discretion prior to the effective date for CIP version 5?

Enforcement discretion is the ability of NERC and Regional Entities to decline to pursue instances of noncompliance with Reliability Standards. Noncompliance that is not pursued through an enforcement action is recorded as a compliance exception. During 2014, NERC and the Regional Entities are exercising enforcement discretion over minimal risk noncompliance arising out of specific entities, selected to participate in the program. There is no application process for enforcement discretion. NERC and the Regional Entities are expanding the program gradually during 2014 and expect that enforcement discretion will apply to minimal risk noncompliance from any registered entity in 2015.

Frequently Asked Questions

'Identify, Assess, Correct' (IAC) and the Reliability Assurance Initiative (RAI)

14. Illustrate the continuum across CIP Standards, NERC Compliance and NERC Enforcement under RAI including the entity obligations and tools used within the different divisions.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement Reminder

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Ballots and Non-Binding Polls Now Open through July 16, 2014

Now Available

Ballots for **Critical Infrastructure Protection Standards Version 5 Revisions** and Non-Binding Polls of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) are open through **8 p.m. Eastern on Wednesday, July 16, 2014.**

There are ballots and non-binding polls set-up as follows:

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel and Training
- CIP-006-6 — Cyber Security — Physical Security
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-2 — Cyber Security — Configuration Change Management
- CIP-011-2 — Cyber Security — Information Protection

There is also a ballot for the Definition of Terms Used in the standards.

If you have questions please contact Ryan Stewart or Marisa Hecht.

Background information for this project can be found on the project page.

Instructions for Balloting

Members of the ballot pools associated with this project may log in and submit their vote for the standards and non-binding polls of the associated VRFs and VSLs by clicking here.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standards. If the comments do not show the need for significant revisions, the standards will proceed to a final ballot.

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Formal Comment Period Now Open through July 16, 2014
Ballot Pools Forming Now through July 1, 2014

Now Available

A 45-day formal comment period for **Critical Infrastructure Protection Standards Version 5 Revisions** is open through **8 p.m. Eastern on Wednesday, July 16, 2014.**

If you have questions please contact Ryan Stewart or Marisa Hecht.

Background information for this project can be found on the project page.

Instructions for Commenting

Please use the electronic form to submit comments on the standards. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for the ballots of the standards and the associated non-binding polls on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Ballot: bp-2014-02 CIPV5_STDS_in@nerc.com
Non-Binding poll: bp-2014-02 CIPV5_NB_in@nerc.com

Please note: To avoid the inconvenience for the industry to join 15 separate ballot pools, we have set up one for the ballots (on the standards and definition) and one for the non-binding polls. Once the ballot pools close, individual ballots will be created by carrying over the members of the ballot pools. There will be a separate ballot for each of the 7 standards, the definition and 7 non-binding polls.

Next Steps

Ballots for the standards, definition and non-binding polls of the associated VRFs and VSLs will be conducted **July 7-16, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Formal Comment Period Now Open through July 16, 2014
Ballot Pools Forming Now through July 1, 2014

Now Available

A 45-day formal comment period for **Critical Infrastructure Protection Standards Version 5 Revisions** is open through **8 p.m. Eastern on Wednesday, July 16, 2014.**

If you have questions please contact Ryan Stewart or Marisa Hecht.

Background information for this project can be found on the project page.

Instructions for Commenting

Please use the electronic form to submit comments on the standards. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for the ballots of the standards and the associated non-binding polls on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Ballot: bp-2014-02 CIPV5_STDS_in@nerc.com
Non-Binding poll: bp-2014-02 CIPV5_NB_in@nerc.com

Please note: To avoid the inconvenience for the industry to join 15 separate ballot pools, we have set up one for the ballots (on the standards and definition) and one for the non-binding polls. Once the ballot pools close, individual ballots will be created by carrying over the members of the ballot pools. There will be a separate ballot for each of the 7 standards, the definition and 7 non-binding polls.

Next Steps

Ballots for the standards, definition and non-binding polls of the associated VRFs and VSLs will be conducted **July 7-16, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Ballot and Non-Binding Poll Results

Now Available

Ballots for seven standards - **Critical Infrastructure Protection Version 5 Revisions** and one definition; and seven non-binding polls of the associated Violation Risk Factors and Violation Severity Levels concluded at **8 p.m. Eastern on Wednesday, July 16, 2014**.

Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballots.

	Ballot Results	Non-Binding Poll Results
	Quorum /Approval	Quorum/Supportive Opinions
CIP-003-6	80.73% / 35.67%	77.81% / 31.86%
CIP-004-6	80.49% / 80.76%	77.27% / 77.63%
CIP-006-6	80.00% / 76.24%	77.27% / 74.56%
CIP-007-6	80.24% / 78.41%	77.27% / 75.44%
CIP-009-6	80.24% / 85.32%	77.27% / 85.59%
CIP-010-2	80.49% / 49.42%	77.54% / 39.04%
CIP-011-2	80.24% / 82.55%	77.01% / 79.74%
Definition	78.29% / 78.58%	N/A

Background information for this project can be found on the project page.

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standards and post them for an additional ballot. If the comments do not show the need for significant revisions, the standards will proceed to a final ballot.

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller (via email), Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2014-02 CIP-003-6 July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	331
Total Ballot Pool:	410
Quorum:	**80.73 % The Quorum has been reached**
Weighted Segment Vote:	35.67 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	22	0.247	67	0.753	1	7	16
2 - Segment 2	9	0.6	5	0.5	1	0.1	0	2	1
3 - Segment 3	93	1	14	0.187	61	0.813	0	3	15
4 - Segment 4	34	1	5	0.227	17	0.773	0	2	10
5 - Segment 5	91	1	14	0.215	51	0.785	0	1	25
6 - Segment 6	54	1	11	0.25	33	0.75	0	1	9
7 - Segment 7	2	0.1	0	0	1	0.1	0	0	1
8 - Segment 8	5	0.3	2	0.2	1	0.1	0	1	1
9 - Segment 9	2	0.1	0	0	1	0.1	0	0	1

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**6.8**	**79**	**2.426**	**234**	**4.374**	**1**	**17**	**79**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz - AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
1	Avista Utilities	Heather Rosentrater	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Balancing Authority of Northern California	Kevin Smith	Negative	SUPPORTS THIRD PARTY COMMENTS- LPPC/SMUD
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
1	City of Tallahassee	Daniel S Langston	Negative	COMMENT RECEIVED
1	Clark Public Utilities	Jack Stamper	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
1	Colorado Springs Utilities	Shawna Speer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Reference Comments - Colorado Springs

				Utilities)
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Doug E Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	Empire District Electric Co.	Ralph F Meyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Kalem Long Empire)
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Negative	COMMENT RECEIVED
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Negative	SUPPORTS THIRD PARTY COMMENTS - (Ayesha Sabouba)
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Negative	COMMENT RECEIVED
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
				SUPPORTS THIRD PARTY

1	M & A Electric Power Cooperative	William Price	Negative	COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (National Grid supports NPCC's comments.)
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NPPD comments)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Negative	COMMENT RECEIVED
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Negative	COMMENT RECEIVED
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz (American Electric Power))
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Negative	COMMENT RECEIVED
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders SMUD)
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
				SUPPORTS THIRD PARTY COMMENTS -

1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	(PPL NERC Registered Affiliates)
1	Public Service Company of New Mexico	Laurie Williams	Negative	COMMENT RECEIVED
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Public Service Enterprise Group (PSEG) comments)
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	COMMENT RECEIVED
1	Salt River Project	Robert Kondziolka	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
1	San Diego Gas & Electric	Will Speer	Negative	COMMENT RECEIVED
1	Seattle City Light	Pawel Krupa	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seattle City Light Paul Haase's Comments)
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (Adopt NRECA Comments)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES and NRECA)
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Negative	NO COMMENT RECEIVED
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Michael Hill)
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	

1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI and NPCC)
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar - Megan Wagner)
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Amy Causcelli, Xcel Energy)
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Negative	COMMENT RECEIVED
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power (AEP))
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Negative	COMMENT RECEIVED
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	COMMENT RECEIVED
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Heather Rosentrater)
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas

				Standifur)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	COMMENT RECEIVED
3	City of Redding	Bill Hughes	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD, LPPC)
3	City of Tallahassee	Bill R Fowler	Negative	COMMENT RECEIVED
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Shannon Fair)
3	ComEd	John Bee	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Negative	COMMENT RECEIVED
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Negative	COMMENT RECEIVED
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY COMMENTS - (Associated Electric)

3	Kansas City Power & Light Co.	Joshua D Bach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Negative	COMMENT RECEIVED
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC RSC)
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments)
3	New York Power Authority	David R Rivera	Negative	COMMENT RECEIVED
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Negative	COMMENT RECEIVED
3	Platte River Power Authority	Terry L Baker	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders)
3	PNM Resources	Michael Mertz	Negative	COMMENT RECEIVED
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	COMMENT RECEIVED
3	Salt River Project	John T. Underhill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seattle City Light Paul Haase's Comments)
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Negative	SUPPORTS THIRD PARTY COMMENTS- LPPC, MIKE HILL - (LPPC)
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (TVA electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
				SUPPORTS

3	Westar Energy	Bo Jones	Negative	THIRD PARTY COMMENTS - (Westar Energy)
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
4	City of Redding	Nicholas Zettel	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD, LPPC)
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duane Radzwion)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
4	Georgia System Operations Corporation	Guy Andrews	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
4	Herb Schrayshuen	Herb Schrayshuen	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by Florida Municipal Power Agency

				(FMPA).)
4	Integrys Energy Group, Inc.	Christopher Plante	Negative	SUPPORTS THIRD PARTY COMMENTS - (T. Breene will be providing comments for Wisconsin Public Service Corp)
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	COMMENT RECEIVED
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	COMMENT RECEIVED
4	Seattle City Light	Hao Li	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seattle City Light Paul Haase's Comments)
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
4	Utility Services, Inc.	Brian Evans-Mongeon	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI comments)
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	SUPPORTS THIRD PARTY COMMENTS - (SCL comments)
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
				SUPPORTS THIRD PARTY

5	City of Redding	Paul A. Cummings	Negative	COMMENTS - (SMUD, LPPC)
5	City of Tallahassee	Karen Webb	Negative	COMMENT RECEIVED
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - (Colorado Springs Utilities)
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
5	Ingleside Cogeneration LP	Michelle R DAntuono	Negative	SUPPORTS THIRD PARTY COMMENTS - (Occidental Chemical Corporation)
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida

				Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Negative	COMMENT RECEIVED
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA Comments submitted by D. Rivera)
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Melvin on behalf of Jerry Freese comments.)
5	Oglethorpe Power Corporation	Bernard Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting EEI's comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	Pacific Gas and Electric Company	Alex Chua	Negative	SUPPORTS THIRD PARTY COMMENTS - (John Hagen, PG&E)
5	Platte River Power Authority	Christopher R Wood	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(PSEG comments)
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Negative	COMMENT RECEIVED
5	Salt River Project	William Alkema	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Negative	COMMENT RECEIVED
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southern Company)
5	Southern Indiana Gas and Electric Co.	Rob Collins	Negative	COMMENT RECEIVED
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
5	Tampa Electric Co.	RJames Rocha	Negative	SUPPORTS THIRD PARTY COMMENTS - (Beth Young)
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Westar Energy	Bryan Taggart	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar Energy)
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Negative	COMMENT RECEIVED
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
				COMMENT

6	Bonneville Power Administration	Brenda S. Anderson	Negative	RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
6	City of Redding	Marvin Briggs	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD, LPPC)
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Negative	SUPPORTS THIRD PARTY COMMENTS - (CSU Comments)
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Negative	COMMENT RECEIVED
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
6	New York Power Authority	Shivaz Chopra	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC RSC)
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (GTC)
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
				COMMENT

6	PacifiCorp	Sandra L Shaffer	Negative	RECEIVED
6	Platte River Power Authority	Carol Ballantine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders with SMUD)
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Negative	COMMENT RECEIVED
6	Salt River Project	William Abraham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Negative	SUPPORTS THIRD PARTY COMMENTS - (Paul Haase)
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (Adopt NRECA's comments)
6	Snohomish County PUD No. 1	Kenn Backholm	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Negative	COMMENT RECEIVED
6	Tacoma Public Utilities	Michael C Hill	Negative	COMMENT RECEIVED
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Refer to comments submitted by Beth Young)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Negative	COMMENT RECEIVED
7	Occidental Chemical	Venona Greaff	Negative	COMMENT RECEIVED
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
8		Debra R Warner		
8		David L Kiguel	Abstain	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts	Donald Nelson	Negative	SUPPORTS THIRD PARTY

	Department of Public Utilities			COMMENTS - (NPCC)
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	COMMENT RECEIVED
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-004-6 July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	330
Total Ballot Pool:	410
Quorum:	**80.49 % The Quorum has been reached**
Weighted Segment Vote:	80.76 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	67	0.77	20	0.23	0	9	17
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	52	0.712	21	0.288	0	5	15
4 - Segment 4	34	1	16	0.727	6	0.273	0	2	10
5 - Segment 5	91	1	43	0.694	19	0.306	0	4	25
6 - Segment 6	54	1	33	0.75	11	0.25	0	1	9
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.7	7	0.7	0	0	0	0	0
Totals	**410**	**7**	**231**	**5.653**	**77**	**1.347**	**0**	**22**	**80**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz - AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Negative	COMMENT RECEIVED
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	COMMENT RECEIVED
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		

1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Negative	COMMENT RECEIVED
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NPPD comments)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz (American Electric Power))
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Public Service Enterprise Group (PSEG) comments)
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	

1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Michael Hill)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power (AEP))
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Heather

				Rosentrater)
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Negative	COMMENT RECEIVED
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments.)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments)
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC and Mike Hill)
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
				SUPPORTS

3	Wisconsin Electric Power Marketing	James R Keller	Negative	THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duane Radzwion)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	

4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Negative	COMMENT RECEIVED
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	

5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Melvin on behalf of Jerry Freese comments.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS - (PSEG Comments)
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin

				Electric Power Co. and EEI)
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)

6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	COMMENT RECEIVED
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-006-6 July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	328
Total Ballot Pool:	410
Quorum:	**80.00 % The Quorum has been reached**
Weighted Segment Vote:	76.24 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	65	0.739	23	0.261	0	8	17
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	49	0.671	24	0.329	0	4	16
4 - Segment 4	34	1	16	0.727	6	0.273	0	2	10
5 - Segment 5	91	1	40	0.635	23	0.365	0	3	25
6 - Segment 6	54	1	31	0.689	14	0.311	0	0	9
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.6	5	0.5	1	0.1	0	0	1
Totals	**410**	**6.9**	**219**	**5.261**	**91**	**1.639**	**0**	**18**	**82**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Kalem Long Empire)
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	SUPPORTS THIRD PARTY COMMENTS - (NextEra Energy)
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	

1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NPPD comments)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standard Review Group)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	

1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (Adopt NRECA Comments)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Amy Causcelli, Xcel Energy)
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
				SUPPORTS THIRD PARTY

3	Avista Corp.	Scott J Kinney	Negative	COMMENTS - (Heather Rosentrater)
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer		
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments.)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Negative	COMMENT RECEIVED
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
				SUPPORTS

3	Kissimmee Utility Authority	Gregory D Woessner	Negative	THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments)
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		

3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (TVA electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duane Radzwion)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency)
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		

4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED

5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	SUPPORTS THIRD PARTY COMMENTS - (NextEra Energy)
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting SPP's comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	

5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Negative	SUPPORTS THIRD PARTY COMMENTS - (Beth Young)
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Negative	COMMENT RECEIVED
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Negative	SUPPORTS THIRD PARTY COMMENTS - (NextEra Energy)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	

6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (support NRECA's comments)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Refer to comments submitted by Beth Young)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Negative	COMMENT RECEIVED
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-007-6 July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	329
Total Ballot Pool:	410
Quorum:	**80.24 % The Quorum has been reached**
Weighted Segment Vote:	78.41 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	62	0.713	25	0.287	0	9	17
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	45	0.616	28	0.384	0	5	15
4 - Segment 4	34	1	15	0.682	7	0.318	0	2	10
5 - Segment 5	91	1	45	0.726	17	0.274	0	4	25
6 - Segment 6	54	1	34	0.773	10	0.227	0	1	9
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.6	6	0.6	0	0	0	0	1
Totals	**410**	**6.9**	**220**	**5.41**	**87**	**1.49**	**0**	**22**	**81**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz -- AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Negative	COMMENT RECEIVED
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	

1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NPPD comments)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz (American Electric Power))
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		

1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (Adopt NRECA Comments)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI and NPCC)
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American

				Electric Power (AEP))
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Heather Rosentrater)
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments.)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
				SUPPORTS THIRD PARTY

3	Gainesville Regional Utilities	Kenneth Simmons	Negative	COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY COMMENTS - (Assoicated Electric)
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments)
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	

3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (TVA electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duane Radzwion)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
				SUPPORTS THIRD PARTY

4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante	Negative	SUPPORTS THIRD PARTY COMMENTS - (T Breene, Wisconsin Public Service Corp)
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		

5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	

5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
				SUPPORTS THIRD PARTY

6	Lakeland Electric	Paul Shipps	Negative	COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-009-6 July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	329
Total Ballot Pool:	410
Quorum:	**80.24 % The Quorum has been reached**
Weighted Segment Vote:	85.32 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	73	0.839	14	0.161	0	9	17
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	56	0.767	17	0.233	0	5	15
4 - Segment 4	34	1	17	0.773	5	0.227	0	2	10
5 - Segment 5	91	1	49	0.79	13	0.21	0	4	25
6 - Segment 6	54	1	36	0.818	8	0.182	0	1	9
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.6	6	0.6	0	0	0	0	1
Totals	**410**	**6.9**	**250**	**5.887**	**57**	**1.013**	**0**	**22**	**81**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Negative	COMMENT RECEIVED
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion's)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
				SUPPORTS THIRD PARTY

1	Lakeland Electric	Larry E Watt	Negative	COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Negative	COMMENT RECEIVED
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NPPD comments)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Public Service Enterprise Group (PSEG) comments)
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)

1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Heather Rosentrater)
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	

3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments.)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments)
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)

3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (TVA electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duane Radzwion)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	

4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	

5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS - (PSEG Comments)
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	

5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT

				RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Ballot Results	
Ballot Name:	Project 2014-02 CIP-010-2 July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	330
Total Ballot Pool:	410
Quorum:	**80.49 % The Quorum has been reached**
Weighted Segment Vote:	49.42 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	31	0.348	58	0.652	0	8	16
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	23	0.311	51	0.689	0	4	15
4 - Segment 4	34	1	5	0.227	17	0.773	0	2	10
5 - Segment 5	91	1	19	0.306	43	0.694	0	4	25
6 - Segment 6	54	1	14	0.318	30	0.682	0	1	9
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.6	6	0.6	0	0	0	0	1
Totals	**410**	**6.9**	**111**	**3.41**	**199**	**3.49**	**0**	**20**	**80**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz - AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
1	Avista Utilities	Heather Rosentrater	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Balancing Authority of Northern California	Kevin Smith	Negative	SUPPORTS THIRD PARTY COMMENTS- LPPC/SMUD
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion's)

1	Duke Energy Carolina	Doug E Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Negative	COMMENT RECEIVED
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	

1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NPPD comments)
1	Network & Security Technologies	Nicholas Lauriat	Negative	COMMENT RECEIVED
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz (American Electric Power))
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Negative	COMMENT RECEIVED
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders SMUD)
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
1	Public Service Company of New Mexico	Laurie Williams	Negative	COMMENT RECEIVED
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	COMMENT RECEIVED
1	Salt River Project	Robert Kondziolka	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
1	San Diego Gas & Electric	Will Speer	Negative	COMMENT RECEIVED
				SUPPORTS THIRD PARTY

1	Seattle City Light	Pawel Krupa	Negative	COMMENTS - (Seattle City Light Paul Haase's Comments)
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES and NRECA)
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Michael Hill)
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI and NPCC)
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar - Megan Wagner)
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Amy Causcelli, Xcel Energy)
2	BC Hydro	Venkataramakrishnan Vinnakota		

2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power (AEP))
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Negative	COMMENT RECEIVED
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Heather Rosentrater)
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD, LPPC)
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	

3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments.)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy comments)
3	Florida Keys Electric Cooperative	Tom B Anthony	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY COMMENTS - (Associated Electric)
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican

				Energy Company)
3	Modesto Irrigation District	Jack W Savage	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments)
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NRECA comments)
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Negative	COMMENT RECEIVED
3	Platte River Power Authority	Terry L Baker	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders)
3	PNM Resources	Michael Mertz	Negative	COMMENT RECEIVED
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	COMMENT RECEIVED
3	Salt River Project	John T. Underhill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
3	Santee Cooper	James M Poston	Affirmative	

3	Seattle City Light	Dana Wheelock	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seattle City Light Paul Haase's Comments)
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC and Mike Hill)
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (TVA electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar Energy)
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
4	City of Redding	Nicholas Zettel	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD, LPPC)
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duane Radzwion)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
				SUPPORTS

4	Flathead Electric Cooperative	Russ Schneider	Negative	THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
4	Georgia System Operations Corporation	Guy Andrews	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municpal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante	Negative	SUPPORTS THIRD PARTY COMMENTS - (T Breene, Wisconsin Public Service Corp)
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	COMMENT RECEIVED
4	North Carolina Electric Membership Corp.	John Lemire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy Comments)
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	COMMENT RECEIVED
4	Seattle City Light	Hao Li	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seattle City Light Paul Haase's Comments)
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
				SUPPORTS

4	Tacoma Public Utilities	Keith Morisette	Negative	THIRD PARTY COMMENTS - (Mike Hill)
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI comments)
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	SUPPORTS THIRD PARTY COMMENTS - (SCL comments)
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
5	City of Redding	Paul A. Cummings	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD, LPPC)
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)

5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy's Comments)
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Luminant Generation Company LLC	Rick Terrill	Negative	SUPPORTS THIRD PARTY COMMENTS - (LUminant Energy Company LLC)
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Melvin on behalf of Jerry Freese comments.)
5	Oglethorpe Power Corporation	Bernard Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting EEI's

				comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	Pacific Gas and Electric Company	Alex Chua	Negative	SUPPORTS THIRD PARTY COMMENTS - (John Hagen, PG&E)
5	Platte River Power Authority	Christopher R Wood	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders (SMUD))
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Negative	COMMENT RECEIVED
5	Salt River Project	William Alkema	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southern Company)
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
5	Tampa Electric Co.	RJames Rocha	Negative	SUPPORTS THIRD PARTY COMMENTS - (Beth Young)
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Westar Energy	Bryan Taggart	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar Energy)
				SUPPORTS

5	Wisconsin Electric Power Co.	Linda Horn	Negative	THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
6	City of Redding	Marvin Briggs	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD, LPPC)
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon Exelon Companies)
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
6	FirstEnergy Solutions	Kevin Querry	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
6	Luminant Energy	Brenda Hampton	Negative	COMMENT RECEIVED
6	Manitoba Hydro	Blair Mukanik	Affirmative	

6	Modesto Irrigation District	James McFall	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (GTC)
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders with SMUD)
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Negative	COMMENT RECEIVED
6	Salt River Project	William Abraham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Negative	SUPPORTS THIRD PARTY COMMENTS - (Paul Haase)
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
6	Snohomish County PUD No. 1	Kenn Backholm	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	COMMENT RECEIVED
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Refer to comments submitted by Beth Young)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Abstain	

7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-011-2 July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	329
Total Ballot Pool:	410
Quorum:	**80.24 % The Quorum has been reached**
Weighted Segment Vote:	82.55 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	68	0.782	19	0.218	0	9	17
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	50	0.685	23	0.315	0	5	15
4 - Segment 4	34	1	15	0.682	7	0.318	0	2	10
5 - Segment 5	91	1	50	0.806	12	0.194	0	4	25
6 - Segment 6	54	1	37	0.841	7	0.159	0	1	9
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.6	6	0.6	0	0	0	0	1
Totals	**410**	**6.9**	**239**	**5.696**	**68**	**1.204**	**0**	**22**	**81**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Negative	COMMENT RECEIVED
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion's)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	

1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Negative	COMMENT RECEIVED
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NPPD comments)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Public Service Enterprise Group (PSEG) comments)
	Public Utility District No. 1 of Okanogan			

1	County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Heather Rosentrater)
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)

3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments.)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY COMMENTS - (Associated Electric)
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments)
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo,

				Wisconsin Electric Power Co. and EEI)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duane Radzwion)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante	Negative	SUPPORTS THIRD PARTY COMMENTS - (T Breene, Wisconsin Public Service Corp)
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	

4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	

5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS - (PSEG Comments)
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo, Wisconsin Electric Power Co. and EEI)
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	

6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	

8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 Definition July 2014_in
Ballot Period:	7/7/2014 - 7/16/2014
Ballot Type:	Initial
Total # Votes:	321
Total Ballot Pool:	410
Quorum:	**78.29 % The Quorum has been reached**
Weighted Segment Vote:	78.58 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	57	0.687	26	0.313	0	10	20
2 - Segment 2	9	0.8	7	0.7	1	0.1	0	0	1
3 - Segment 3	93	1	49	0.69	22	0.31	0	4	18
4 - Segment 4	34	1	16	0.762	5	0.238	0	3	10
5 - Segment 5	91	1	44	0.733	16	0.267	0	4	27
6 - Segment 6	54	1	33	0.75	11	0.25	0	1	9
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	1	1
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.6	6	0.6	0	0	0	0	1
Totals	**410**	**6.9**	**217**	**5.422**	**81**	**1.478**	**0**	**23**	**89**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion's)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Kalem Long Empire, and EEI)
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Negative	COMMENT RECEIVED
1	Great River Energy	Gordon Pietsch	Affirmative	

1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan		
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	COMMENT RECEIVED
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
				SUPPORTS

1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	THIRD PARTY COMMENTS - (NRECA)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES and NRECA)
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Michael Hill)
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar - Megan Wagner)
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Negative	COMMENT RECEIVED
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Negative	COMMENT RECEIVED
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	

3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney		
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Dominion's submitted comments.)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia System Operations)
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
				SUPPORTS

3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	THIRD PARTY COMMENTS - (AECI)
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman		
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NRECA comments)
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Negative	COMMENT RECEIVED
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	COMMENT RECEIVED
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperatve)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC and Mike Hill)
3	Tampa Electric Co.	Ronald L. Donahey		
				SUPPORTS

3	Tennessee Valley Authority	Ian S Grant	Negative	THIRD PARTY COMMENTS - (TVA electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar Energy)
3	Wisconsin Electric Power Marketing	James R Keller		
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Negative	SUPPORTS THIRD PARTY COMMENTS - (T Breene, Wisconsin Public Service Corp)
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	COMMENT RECEIVED
4	North Carolina Electric Membership Corp.	John Lemire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	

5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
				SUPPORTS THIRD PARTY

5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	COMMENTS - (Mike Melvin on behalf of Jerry Freese comments.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting EEI's comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Abstain	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Negative	COMMENT RECEIVED
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southern Company)
5	Southern Indiana Gas and Electric Co.	Rob Collins		
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
5	Tampa Electric Co.	RJames Rocha	Negative	SUPPORTS THIRD PARTY COMMENTS - (Beth Young)
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar Energy)
5	Wisconsin Electric Power Co.	Linda Horn		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
				SUPPORTS THIRD PARTY

6	Cleco Power LLC	Robert Hirchak	Negative	COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	COMMENT RECEIVED
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Refer to comments submitted by Beth Young)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Abstain	

8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-003-6
Poll Period:	7/7/2014 - 7/16/2014
Total # Opinions:	291
Total Ballot Pool:	374
Summary Results:	77.81% of those who registered to participate provided an opinion or an abstention; 31.86% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
1	Avista Utilities	Heather Rosentrater	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Negative	COMMENT RECEIVED
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)

1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Negative	COMMENT RECEIVED
1	Clark Public Utilities	Jack Stamper	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
1	Colorado Springs Utilities	Shawna Speer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Reference Comments - Colorado Springs Utilities)
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Negative	SUPPORTS THIRD PARTY COMMENTS - (Ayesha Sabouba)
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (NPCC)
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Abstain	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Abstain	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (National Grid supports

				NPCC's comments.)
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Negative	COMMENT RECEIVED
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Negative	COMMENT RECEIVED
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Negative	COMMENT RECEIVED
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	COMMENT RECEIVED
1	Salt River Project	Robert Kondziolka	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)

1	San Diego Gas & Electric	Will Speer	Negative	COMMENT RECEIVED
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES and NRECA)
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Michael Hill)
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(Westar - Megan Wagner)
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Negative	COMMENT RECEIVED
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Abstain	
3	American Public Power Association	Nathan Mitchell		
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	

3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Tallahassee	Bill R Fowler	Negative	COMMENT RECEIVED
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Shannon Fair)
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Negative	COMMENT RECEIVED
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Associated Electric)
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Abstain	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Abstain	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC RSC)
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Negative	COMMENT RECEIVED
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)

3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	COMMENT RECEIVED
3	Salt River Project	John T. Underhill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(LPPC and Mike Hill)
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar Energy)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifu)
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American

				Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante		
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	COMMENT RECEIVED
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	SUPPORTS THIRD PARTY COMMENTS - (SCL comments)
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
5	City of Tallahassee	Karen Webb	Negative	COMMENT RECEIVED
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - (Colorado Springs Utilities)
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (NPCC)
5	Ingleside Cogeneration LP	Michelle R DAntuono	Negative	SUPPORTS THIRD PARTY COMMENTS - (Occidental Chemical Corporation)
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Abstain	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SMUD)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA Comments submitted by D. Rivera)
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Mike Melvin on behalf of Jerry Freese comments.)
5	Oglethorpe Power Corporation	Bernard Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting EEI's comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Negative	SUPPORTS THIRD PARTY COMMENTS - (John Hagen, PG&E)
5	Platte River Power Authority	Christopher R Wood	Abstain	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Negative	COMMENT RECEIVED
5	Salt River Project	William Alkema	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)

5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southern Company)
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
5	Tampa Electric Co.	RJames Rocha	Negative	SUPPORTS THIRD PARTY COMMENTS - (Beth Young)
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Abstain	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Negative	SUPPORTS THIRD PARTY COMMENTS - (CSU Comments)
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(Duke Energy)
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Abstain	
6	New York Power Authority	Shivaz Chopra	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC RSC)
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (GTC)
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders with SMUD)
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC

				Registered Affiliates)
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	COMMENT RECEIVED
6	Salt River Project	William Abraham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Negative	SUPPORTS THIRD PARTY COMMENTS - (Paul Haase)
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
6	Snohomish County PUD No. 1	Kenn Backholm	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Tacoma Public Utilities	Michael C Hill	Negative	COMMENT RECEIVED
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Refer to comments submitted by Beth Young)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Negative	COMMENT RECEIVED
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
8		Debra R Warner		
8		David L Kiguel	Abstain	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	

9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	COMMENT RECEIVED
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-004-6
Poll Period:	7/7/2014 - 7/16/2014
Total # Opinions:	289
Total Ballot Pool:	374
Summary Results:	77.27% of those who registered to participate provided an opinion or an abstention; 77.63% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Negative	COMMENT RECEIVED
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	

1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	

1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	

1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Michael Hill)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Abstain	
3	American Public Power Association	Nathan Mitchell		
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	

3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Tallahassee	Bill R Fowler	Negative	COMMENT RECEIVED
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (LPPC and Mike Hill)
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency)
4	Integrys Energy Group, Inc.	Christopher Plante		
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		

4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Negative	COMMENT RECEIVED
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	

5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Melvin on behalf of Jerry Freese comments.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Abstain	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	

5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein		
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	

6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	COMMENT RECEIVED
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		

6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-006-6
Poll Period:	7/7/2014 - 7/16/2014
Total # Opinions:	289
Total Ballot Pool:	374
Summary Results:	77.27% of those who registered to participate provided an opinion or an abstention; 74.56% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		

1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	SUPPORTS THIRD PARTY COMMENTS - (NextEra Energy)
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (MidAmerican Energy)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Abstain	
3	American Public Power Association	Nathan Mitchell		
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		

3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Negative	COMMENT RECEIVED
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)

3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power

				Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante		
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	

5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	SUPPORTS THIRD PARTY COMMENTS - (NextEra Energy)
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	

5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting SPP's comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Abstain	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Negative	SUPPORTS THIRD PARTY COMMENTS - (Beth Young)
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein		
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	

6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Negative	SUPPORTS THIRD PARTY COMMENTS - (NextEra Energy)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	

6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Refer to comments submitted by Beth Young)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-007-6
Poll Period:	7/7/2014 - 7/16/2014
Total # Opinions:	289
Total Ballot Pool:	374
Summary Results:	77.27% of those who registered to participate provided an opinion or an abstention; 75.44% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	

1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Sho-Me Power Electric Cooperative	Denise Stevens		

1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Abstain	
3	American Public Power Association	Nathan Mitchell		
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	

3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Associated Electric)
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	

3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	

4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante		
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		

5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	

5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Abstain	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein		
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Abstain	

6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	

6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-009-6
Poll Period:	7/7/2014 - 7/16/2014
Total # Opinions:	289
Total Ballot Pool:	374
Summary Results:	77.27% of those who registered to participate provided an opinion or an abstention; 85.59% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	

1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	

1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda Shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED

1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Abstain	
3	American Public Power Association	Nathan Mitchell		
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	

3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	

3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency)
4	Integrys Energy Group, Inc.	Christopher Plante		
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	

5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	

5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Abstain	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein		
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED

6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	

6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-010-2
Poll Period:	7/7/2014 - 7/16/2014
Total # Opinions:	290
Total Ballot Pool:	374
Summary Results:	77.54% of those who registered to participate provided an opinion or an abstention; 39.04% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
1	Avista Utilities	Heather Rosentrater	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Negative	COMMENT RECEIVED
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)

1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPPC)
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Abstain	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)

1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Negative	COMMENT RECEIVED
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	COMMENT RECEIVED
1	Salt River Project	Robert Kondziolka	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
1	San Diego Gas & Electric	Will Speer	Negative	COMMENT RECEIVED
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda shumpert)

1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES and NRECA)
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Michael Hill)
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar - Megan Wagner)
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	

2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Abstain	
3	American Public Power Association	Nathan Mitchell		
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		

3	FirstEnergy Corp.	Cindy E Stewart	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy Comments)
3	Florida Keys Electric Cooperative	Tom B Anthony	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY COMMENTS - (Associated Electric)
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)

3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Abstain	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support NRECA comments)
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien on behalf of Jerry Freese)
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)

3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	COMMENT RECEIVED
3	Salt River Project	John T. Underhill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Negative	SUPPORTS THIRD PARTY COMMENTS - (LPCC and Mike Hill)
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (Westar Energy)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	SUPPORTS THIRD PARTY COMMENTS - (Standifur)
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	

4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante		
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy Comments)
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal

				Utility District)
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	COMMENT RECEIVED
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	SUPPORTS THIRD PARTY COMMENTS - (SCL comments)
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	

5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy's Comments)
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Luminant Generation Company LLC	Rick Terrill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Luminant Energy

				Company LLC)
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Melvin on behalf of Jerry Freese comments.)
5	Oglethorpe Power Corporation	Bernard Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Georgia Transmission Corp)
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting SPP's comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Negative	SUPPORTS THIRD PARTY COMMENTS - (John Hagen, PG&E)
5	Platte River Power Authority	Christopher R Wood	Abstain	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		

5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Negative	COMMENT RECEIVED
5	Salt River Project	William Alkema	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southern Company)
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mike Hill)
5	Tampa Electric Co.	RJames Rocha	Negative	SUPPORTS THIRD PARTY COMMENTS - (Beth Young)
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein		
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		

6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
6	FirstEnergy Solutions	Kevin Querry	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Negative	SUPPORTS THIRD PARTY COMMENTS - (SMUD)
6	Luminant Energy	Brenda Hampton	Negative	COMMENT RECEIVED
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Abstain	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (GTC)
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Scott Saunders wtih SMUD)
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	COMMENT RECEIVED
6	Salt River Project	William Abraham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Salt River Project)
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Negative	SUPPORTS THIRD PARTY COMMENTS - (Paul Haase)
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
6	Snohomish County PUD No. 1	Kenn Backholm	Negative	SUPPORTS THIRD PARTY COMMENTS - (Sacramento Municipal Utility District)
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Tacoma Public Utilities	Michael C Hill	Negative	COMMENT RECEIVED
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Refer to

				comments submitted by Beth Young)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-011-2
Poll Period:	7/7/2014 - 7/16/2014
Total # Opinions:	288
Total Ballot Pool:	374
Summary Results:	77.01% of those who registered to participate provided an opinion or an abstention; 79.74% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole		
1	Associated Electric Cooperative, Inc.	John Bussman		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Negative	COMMENT RECEIVED
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	

1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler		
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	

1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	SUPPORTS THIRD PARTY COMMENTS - (Rolynda shumpert)
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	

1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Abstain	
3	American Public Power Association	Nathan Mitchell		
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	COMMENT RECEIVED
3	Central Electric Power Cooperative	Adam M Weber	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		

3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla		
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	SUPPORTS THIRD PARTY COMMENTS - (Associated Electric)
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)

3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	

3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	SUPPORTS THIRD PARTY COMMENTS - (AECI)
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble		
4	Cowlitz County PUD	Rick Syring		
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	SUPPORTS THIRD PARTY COMMENTS - (NRECA)
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency and American Public Power Association)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by Florida

				Municipal Power Agency (FMPA))
4	Integrys Energy Group, Inc.	Christopher Plante		
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski		
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	COMMENT RECEIVED
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	

5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh		
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Abstain	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	

5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein		
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	COMMENT RECEIVED
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Comments)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		

6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner		
8		David L Kiguel	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	

10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer		
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Individual or group. (99 Responses)
Name (68 Responses)
Organization (68 Responses)
Group Name (31 Responses)
Lead Contact (31 Responses)
Question 1 (76 Responses)
Question 1 Comments (83 Responses)
Question 2 (71 Responses)
Question 2 Comments (83 Responses)
Question 3 (70 Responses)
Question 3 Comments (83 Responses)
Question 4 (68 Responses)
Question 4 Comments (83 Responses)
Question 5 (72 Responses)
Question 5 Comments (83 Responses)
Question 6 (72 Responses)
Question 6 Comments (83 Responses)
Question 7 (42 Responses)
Question 7 Comments (83 Responses)
Question 8 (73 Responses)
Question 8 Comments (83 Responses)

Individual
mike albosta
Phillips 66
No
No problem with 2.1, 2.2, 2.3 2.4 - Requiring the user to give a "reason" for accessing does nothing to increase security and would require a rewrite of the system. 2.5 - We just wrote an Incident Response Plan for EOP-004-2 that would cover cyber incidents. This is redundant and more work. 2.6 - ditto. And quarterly is ridiculous. And you don't define "practices" or what "reinforce" means.
Group
FirstEnergy
Cindy Stewart
Yes
FirstEnergy supports the revisions to the CIP standard in general. Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does have concerns around the RSAWs and support EEIs comments in regards to the RSAWs.
Yes
FirstEnergy supports the revisions to the CIP standard in general. However in the Guidelines and Technical Basis, FirstEnergy requests the addition of a clarification that entities are not expected to enforce CIP-006 on third party components that are out of the entity’s control. FirstEnergy also has concerns around the RSAWs and support EEIs comments in regards to the RSAWs.
No

FirstEnergy does not agree with this approach. Suggest the requirements for Transient Cyber Assets & Removable Media Protection be an additional requirement under CIP-007 as these devices require similar protection (i.e. malicious code prevention, security patching) as those applicable systems in CIP-007. As currently placed, Transient Cyber Assets & Removable Media have little in common with Configuration Change Management and Vulnerability Assessments creating confusion in internal programs, SMEs and RSAWs.
Yes
Yes
Yes
No
None known
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does have concerns around the RSAWs and support EEIs comments in regards to the RSAWs.
Individual
Greg Froehling
Rayburn Country Electrical Cooperative
No
The proposed version provides adequate specificity relative to the strategies required. E.g. “restrict physical access”. The concern I pose, comes with the subjective nature of the enforcement review. Does the standard sufficiently cover the appropriate levels and tactics expected to be used to be compliant. (is locking the door enough?) However this COULD be addressed with a sufficiently detailed technical guidance document much like the style of the PRC-005 Technical Guidance Document. Next Section 2.5 needs some language clarification; two intervals are mentioned, quarterly and 15 calendar months. However there is some ambiguity surrounding what is to be done on those intervals. A suggested wording / format revision to clarify. Implement a security awareness program that: •Reinforces good cyber security practices at least quarterly. In addition. •Specifically cover Parts 2.2, 2.3, and 2.4 above, once every 15 calendar months.
No Comment
No Comment
Yes
The timeline for CIP-003-6 R2 should be sufficient. But I point out that the implementation plan does not address newly identified "Low" BES Cyber Assets. The situation could occur for some distribution assets that were not applicable at the time this standard was approved, at a later date rising to the applicability levels and as such needing to implement the "Low" requirements.
Yes
Items for the FAQ document produced by the drafting team. •Suggested approaches for compliance that address the topics in CIP-003-6, Requirement R2, and Parts 2.2 – 2.5. (See PRC-005 Technical guidance document for level of specificity.) •What levels of restrictions for physical access are expected to be performed? (Switchyard/ Substations, Generation facilities and areas within those facilities…) •Explore issues around “2.3.3 Authentication when establishing Dial-up Connectivity, per Cyber Asset capability. The documentation of the capability and or suggested approaches to establishing authentication. •Address implementation period for newly identified LOW BES Cyber Assets, currently there is NONE! •Discuss “Guilt by association” example: a substation classified by entity A as “Medium” has Protection Systems (BES Cyber System) that rely on Entity B’s substation Protection Systems, does this potential Reliability Operating Service provided by Entity B make the Entity B’s station a Medium or not? •Also explore the situation above where Entity B’s substation is a

non BES station. Does this scenario extend to those connected to "Low" substations? For CIP-003 R2, I propose the original 2 years from regulatory approval as it was originally with version 5 since it has taken longer than 3 months from V5 FERC Approval till now. More time is needed due to: •The objective criteria and the specific nature of the processes or program required for these proposed revisions that did not exist prior to now. •Entities are not only required to “develop them”. •Entities must demonstrate they have “implemented them” Please address implementation period for newly identified LOW BES cyber assets. Currently this is a situation that can arise, and without an implementation period being identified it can pose some difficult situations.
Individual
Debra Horvath
Portland General Electric
Yes
Yes
Yes
Yes
No
PGE is concerned about the removal of the ‘identify, assess, and correct’ language from the CIP Version 5 standards. The inclusion of this language in the CIP Version 5 standards was a large part of the reason that the industry voted to pass the standards in the first place. The intention of the IAC language was to address the standards being ‘zero defect’, an intention which FERC supported in order 791. ‘Zero defect’ standards cause undue burden and harm on the industry without supplying a meaningful reliability or security benefit. Rather than remove the IAC language entirely, it would be worthwhile to modify the language to add a qualitative aspect that would be responsive to FERC’s concern that the language is too vague. PGE understands that the Reliability Assurance Initiative may be used to address “zero defect” but its effectiveness remains to be seen. It is preferable to include language within the CIP Version 5 standards to address “zero defect”.
Yes
Yes
Yes
Group
CenterPoint Energy
John Brockhan
No
R2/M2 - Although CenterPoint Energy generally agrees with the approach to meeting the CIP-003 directive, one requirement for low impact assets with objective criteria, the Company questions the deletion of the link back to CIP-002-5, Requirement R1, Part R1.3. The Company recommends the following wording: “Each Responsible Entity for its assets identified in CIP-002-5 Requirement R1, Part 1.3 shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets.”. (The phrase “containing low impact BES Cyber Systems” is not needed as it should be understood after asset identification in CIP-002-5.) CenterPoint Energy also recommends that M2 be revised to reflect the pattern of the other measures in CIP-003. For example, the following wording would be appropriate: “Examples of evidence may include, but are not limited to, applicable documented policies and processes that collectively include each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets and additional evidence to demonstrate implementation as describe in the Measures column of the table.” Alternatively, the SDT may consider the pattern found in other Standards (ex. CIP-007-5/6) and remove the word “any” from the draft measure.

Part 2.4.3 - CenterPoint Energy also requests that the SDT review and consider the use of the term “authentication” versus “access control” in Part 2.4.3 and the supporting Guidelines and Technical Basis. Does the SDT intend for entities to have authentication or access control when establishing Dial-up Connectivity? Although this requirement is to be implemented “per Cyber Asset capability”, CenterPoint Energy proposes that access control is more appropriate and commonly feasible. Part 2.6 - The level of detail in Part 2.6 is above what is required even for High and Medium Impact BES Cyber Systems. CenterPoint Energy recommends that Part 2.6 be revised as follows: “Implement a security awareness program that reinforces cyber security practices (which may include associated physical security practices) at least quarterly.”. Delete the sentence “Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.”.
Yes
No
CenterPoint Energy acknowledges the risks associated with transient devices; however, the Company is concerned with management and documentation to be associated with the requirements for transient devices. CenterPoint Energy considers sustained compliance with the requirements exceptionally challenging or unattainable. CenterPoint Energy also recommends that the examples statement be removed from the Guidelines and Technical Basis on Page 41 – Requirement R4 as it is redundant to the definitions of Transient Cyber Assets and Removable Media.
Yes
Yes
CenterPoint Energy supports this revision approach for IAC. As proposed by NERC, the Company looks forward to the concepts of IAC being implemented within the final framework of the Reliability Assurance Initiative (RAI).
No
The timeframe for CIP-010-2, Requirement R4 is not appropriate. Efforts will be focused on the implementation of CIP Version 5 (High and Medium Impact Assets) through April 1, 2016. After that date, entities will have 1 year to document and implement requirements for Low Impact Assets. Although comprehensive efforts toward CIP Version 5 and the potential of CIP Version 6 compliance are occurring to date, CenterPoint Energy recommends that Registered Entities not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until at least 1 year after the effective date of Reliability Standard CIP-010-2 as it, along with CIP-003-2, is the most complex of the CIP Version 5 revisions.
Group
Arizona Public Service Co
Janet Smith
Yes
Yes
Yes
Yes
Yes
Yes
This is not applicable to AZPS as an entity

No
Group
Northeast Power Coordinating Council
Guy Zito
No
We recommend common control objectives. Language inconsistencies create confusion and compliance risks. Here are some examples: Example 1 – Request a definition (CIP-003-6 Rationale R2 and Part 2.4) of “external routable protocol paths” so that Entities and Auditors clearly understand the differences with External Routable Connectivity. We recommend avoiding the earlier CIP-001 confusion between Facilities and facilities. We believe “external routable protocol paths” creates a similar interpretation risk. Example 2 – security awareness (Part 2.6) is more stringent than the High / Medium in CIP-004-6 R1 Example 3 - the Low Incident Response Plan in Part 2.5 is inconsistent with High / Medium Incident Response Plan in CIP-008-5 R2 Example 4 – policy requirements for Low Impact creates different set of Requirements for Entities with Low, Medium or High. There are inconsistencies in the language of this requirement, which causes confusion to entities. Why is LOW impact rating requirements addressed in this standard versus in the applicable standards such as for High & Medium impact ratings? Example: the security awareness should be addressed in CIP 004 as it is for High & Medium. Whether the all-in-one requirement approach or the spreading out into all the standards approach is taken, the most important thing is that there is consistency between the standards and requirements and maintaining the tiering of activities to the risk.
Yes
Request CIP-007 R1 Part 1.2 Rationale be added to the Guidelines and Technical Basis section. Suggest illustrative examples be included in the Measures and Technical Guidelines so that entities and auditors have the same interpretation.
Yes
Yes
Yes
How does NERC intend to address an internal controls program? What is the time line? Refer to the comment for Question 8.
No
Request a clear, concise table of all proposed Implementation Plan updates. Ensure that all new effective and mandatory dates are after their CIP V5 dates. The current format is confusing. Please provide a clear and consistent time line for implementation of these requirements.
No
Yes
More clarity and scenarios should be provided on how RAI and CIP will work together. The NERC Project 2014-02 CIP Version 5 Revisions Standard Drafting Team should be allowed to help clarify and provide guidance for industry issues and items discovered in the pilots. In particular the following should be addressed by NERC with the SDT representing industry: 1. Transfer Trip: CIP-002-5 R1, ‘transmission stations and substations’ for medium category assets, what some refer to as the “transfer trip” issue. 2. Clarify the term “programmable devices” which is an undefined term open to strongly differing viewpoints. 3. Clarify “effect within 15 minutes” issue and the burden of evidence for proving that something does not exist. Please clarify if diversity vs redundancy can be considered as part of the Entity’s impact assessment (i.e. separate system using a different technology). Recommend adding “or” to CIP-010 R4 Part 4.1.4 to make this Part consistent with CIP-010 R1 Part1.1.1.1. Part 1.1.1 requires a baseline of Operating system(s) (including version) OR firmware where no independent operating system exists; while Part 4.1.4 requires Authorization to include Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability). Part 4.1.4 requires Authorization of both Operating System AND

Firmware for a transient device while Part 1.1.1 requires baseline of Operating System OR firmware. We suggest the proper approach is to retain the OR. When applying R4 to a laptop we normally record the OS and version and not look to the firmware BIOS.
Group
ACES Memebers
Warren Cross
No
In regards to the requirement for physical security (R2.2), the requirement is partially focused on whether one or more processes is documented to restrict physical access. The requirement and measures should be focus on the effectiveness with specific physical access restriction criteria instead of a documented process. Would an entity have to document their processes for each asset if the means of restriction are different? If so, this effort to document each process for each location for each asset would be burdensome and ineffective in restricting physical access.
Yes
Yes
Yes
We are supportive of the approach as long as the Reliability Assurance Initiative is fully implemented by the effective date of these standards.
Yes
We are supportive of the approach as long as the Reliability Assurance Initiative is fully implemented by the effective date of these standards.
Yes
No
No
Group
Pacific Gas and Electric
John Hagen
No
The Requirements proposed in 2.1, 2.2 and 2.3 are sound and apportion appropriate controls for Low Impact Cyber Systems. However, the “external routable protocol paths” language in Requirement 2.4 requires entities Low Impact Cyber Systems to provide and comply with “some form of electronic security perimeter,” regardless of risk to the Bulk Power System/Bulk Electric System. In addition, the language in the context of a CIP program is confusing. On one hand, entities would be required to identify, maintain and comply with “some form of electronic security perimeter” (ESP) for Low Impact rated BES Cyber Systems, yet on the other, CIP Version 5 (or the proposed Revisions) states that “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” This is contradictive at best and should be clarified. And while it is understood that one consideration for this language is a scenario where a Low Impact Cyber System could potentially be compromised and/or utilized to compromise or misuse Medium or High rated Cyber Systems; this should be alleviated considering that Low, Medium and High BES Cyber Systems are inherently designed, deployed and operated with existing physical and electronic controls to deter this. Recommend language changes to address only Low Impact Systems which have direct access to “untrusted” networks (e.g. networks not owned and operated by the entity). Recommend adding language to address Low Impact BES Cyber Systems with “external routable protocol paths” and depending on the path and number of paths, determine the controls such as monitor and control communications, implementation of subnets, and manage external connections using boundary protection devices. Recommend the performance of an annual sampling assessment of such classified systems to determine the state of their security controls.

This sampling could be based on the NERC sampling guidelines or other generally accepted audit principles for security controls with established levels of materiality to provide a threshold or cut-off point.
Yes
Implementing physically secured cabling and alarms to components outside of PSP is an appropriate approach. Also, Part 1.10 mandates an alarm or alert to personnel with 15 minutes of detection. However Part 1.10 does not define timeframe that alert or alarm must be respond to or be investigated by personnel to determine if/how/where breach was attempted. Also recommend that periodic review of the integrity of the implemented physical protection measures and alarm processes remain intact as design and approved as part of CIP Senior Manager sign-off.
No
CIP-010-6 R4.1.4 requires the Entity to “identify and document the Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).” And in 4.6, the Entity is required to “Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4.” For entities that depend on vendors and contract support personnel to maintain the Reliability of the Bulk Electric System, this becomes a great administrative challenge. This requirement becomes dependent upon the number of Transient Devices, the number of vendors, contractors or support personnel, and the type and variance of Transient Cyber Assets and tools used to perform their job duties. The challenge in requiring a baseline of firmware alone far exceeds the vulnerably and risk to the BES Cyber Asset. Recommend changing the language in requirements R4.1.4 and R4.6 to address Entity owned-maintained Transient Devices separately from Vendor or Contracted Support owned-maintained Transient Devices. This allows entities to reasonably develop and implement Administrative and Technical Security Controls for Transient Devices based on risk, yet monitored from a compliance standpoint. Recommend language changes to require “the implementation of a Transient Device Security Baseline for Entity and Vendor/Contracted Support Transient Devices.” This allows Entities to implement controls yet maintain the flexibility to address multiple device types and functions. This also allows Entities and their vendors or contracted support personnel to implement Administrative and Technical controls of Transient Devices based on risk. Recommend language changes to require sampling of Transient Devices Security Baseline. This allows Entities a mechanism for monitoring both Entity and Vendor/Contracted Support personnel owned-maintained Transient Devices. Recommend language changes to require a security policy for Transient Devices which includes a requirement for Transient Devices with direct access to BES Cyber Systems. This allows Entities to establish and implement Administrative Controls for Transient Devices as well as recommend Technical Security Controls in the form of Transient Device Access Portals. Recommend consider a standardized implementation of a Transient Device Security Access Portal which allows vendors to perform their work without directly accessing systems. This would allow Entities Vendors, Contractors and support personnel to use a standardized and document attestation of security baseline for Transient Cyber Assets. Recommend leveraging the NERC Guidance for Secure Interactive Remote Access jump hosts concept for transient devices with remote access capabilities.
Yes
The new definition for Transient Cyber Assets and Removable Media is an appropriate revised definition. However, there may be an issue with scope of applicability related to the 15 minute parameter classification of High BES Cyber Asset and Protected Cyber Assets. The new R4 approach should be required across all components contained within the ESP regardless of classification. Also, it is stated under Requirement "4.1 Authorization shall include 4.1.1 Users, individually or by group/role:". Recommend that authorization should always note individual user and removing "by group/role".
No
The intent to removing the specific 17 requirements related to the "Identify, Assess, and Correct (IAC)" language was to shift focus from addressing specific types of incidents to implementing better practices in identifying risks. This shift may present responsible entity with overly-vague, unclear or not detailed enough scope or definition, compliance obligations, timeframes and requirements resulting in hard to develop and implement auditable processes. Recommend defining clearer requirements, scope definitions and obligations in the NERC Compliance Monitoring and Enforcement Program.

Yes
The existing effective dates for the mentioned standards appear reasonable and appropriate.
No
Yes
In the past references have been made regarding a need to protect High BES Cyber Systems from Electro Magnetic Pulse (EMP) related to solar or intentional anomalies. This has been an ongoing topic of discussion and concern however no direction, requirements, obligation or risk considerations have been made. Recommend providing guidance on whether EMP anomalies should be considered in risk assessments or policies and procedures.
Individual
Joe O'Brien on behalf of Jerry Freese
NIPSCO
No
Although we agree with EEI and the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. 4. Applicability The scope of dispersed generation in the CIP-003-6 Applicability section should be limited and similar to PRC-005. Suggested Revision: Under the Introduction section, 4 Applicability, 4.2 Facilities, add the following statement after 4.2.2 All BES Facilities: “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back the reference to CIP-002-5 Requirement R1.3 in CIP-003-6 R2. 6. Background With the addition of the table to Requirement R2, the Background Section should include a paragraph referencing the tables and the “Applicable Systems” Column to be consistent with the Background section of the other CIP standards with similar tables. Suggested Revision: Add the following paragraph after the first sentence of the CIP-003-6 Background Section 6: “Requirement R2 opens with, ‘Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets.’ The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.” Also, add a paragraph similar to the “‘Applicable Systems’ Columns in Tables:” from other CIP standards into the Background Section 6 for CIP-003-6 for Requirement R2. Requirement R2 Add back the reference to “for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3” to properly set the scope. Also, change the table reference to “CIP-003-6 Policies, Processes, Plans and Programs.” to match the proposed revision to the table title. Suggested Revision: Change R2 to: “Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.” Table Title for Requirement R2 The Table title for Requirement R2 “CIP-003-6 Table R2 – Low Impact Assets” does not match the format of the tables used in the other CIP standards, which focus on the requirements not the applicable systems. Suggested Revision: Change the R2 table title to: “CIP-003-6 Table R2 – Low Impact Asset Policies, Processes, Plans, and Programs” Requirement R2, Part 2.1 An entity may not have a low impact BES Cyber System at a Control Center (R2.3) and therefore R2, Part 2.3 is not applicable. Suggested Revision: Edit text to read “that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 -2.6.” Requirement R2, Subpart 2.4.1 Clarify that an external routable protocol path is “external” to the asset identified in CIP-002-5.1 R Requirement R1, Part 1.3 containing low impact BES Cyber Systems. Suggested Revision: Delete “external” and insert “to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems” such that 2.4.1 becomes: “All routable protocol paths to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems, if any, must be through one or more identified access point(s).” Requirement R2, Subpart 2.4.2 Remove “by default” as it implies

the use of a firewall, which limits access control options. For example, an entity could use access control lists on a router or switch to provide security for traffic control. However, routers and switches do not do this by default. This will allow entities more options on how to accomplish traffic control. Also, include a statement to allow documentation of access permissions individually or by group. Reasons for granting access are included in CIP-005-5 Requirement R1, Part 1.3 for high and medium impact BES Cyber Systems. Documentation for low impact assets individually or by group is consistent with the measure, but as in CIP-005-5 Requirement R1, Part 1.3 should be added to the standard. Suggested Revision: Remove “by default” and add “and document access permission reasons individually or by group” such that 2.4.2 becomes: “For each identified access point, if any, require inbound and outbound access permissions, deny all other access, and document access permission reasons individually or by group.” Requirement R2, Part 2.6 The specificity of what must be covered and having to track two time periods is more prescriptive than the requirements for medium and high impact BES Cyber Systems. The proposed revision uses language from the medium/high impact requirement (CIP-004-R1.1) with the time period adjusted to once every 15 calendar months to differentiate for the lower risk. Cyber security awareness can be addressed during annual training for employees and contractors in addition to other ongoing cyber security awareness communications. Suggested Revision: Remove the references to the subpart requirements as they may not apply to all entities and remove the quarterly requirement such that Part 2.6 becomes: “Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months.” Guidelines and Technical Basis Align the drawings and wording in the guidelines and technical basis with the requirement language.

Yes

(EEI Comments) Guidelines and Technical Basis Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity’s control.

No

We agree with the following EEI comments: Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. Requirement R4, Part 4.1 EEI members are concerned with unnecessary administrative burdens created by Part 4.1. For example, Authorization generally applies to users. A user of a Transient Cyber Asset should be authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. Suggested Revision: EEI does not have a specific revision to suggest to address these concerns; however, we recommend a careful review of the specific concerns and suggestions raised by Registered Entities to help reduce the administrative burden of this part. Requirement R4, Part 4.7 The requirement should be tied together better such that it clearly allows mitigation instead of patching, when justified. Suggested Revision: Condense the language into one sentence to help clarify the requirement. For example: “Evaluate Transient Cyber Assets, within 35 calendar days prior to use, for applicable security patches and take one of the following actions: • Apply the applicable patches, or • Create a dated mitigation plan, or • Revise an existing mitigation plan.” Guidelines and Technical Basis The Part 4.1 guidance conflicts with the “Applicable Systems”. The guidance says the requirement (R4) “applies to any transient devices”, yet the “applicable systems” in the requirements tables are not the transient devices. Suggested Revision: Edit the language under Requirement R4 to: “This Requirement applies to Transient Cyber Assets and Removable Media that will be connected temporarily to an applicable system. Examples of these hardware/software devices include, but are not limited to: • Diagnostic test equipment • Packet sniffers • Devices used for BES Cyber System maintenance • Devices uses for BES Cyber System configuration • Devices used to perform vulnerability assessments” The guidance for Requirement Part 4.1, says “Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets.” Requirement R4, Part 4.1 says “Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances.” (emphasis added) The guidance language

should be edited to be consistent with the standard's requirement. Bullet 2, under Requirement Part 4.1, says "It may be reasonable to have separate Transient Cyber Assets for each impact level." Requirement R4, Part 4.1 is focused on High and Medium Impact BES Cyber Systems, not all BES Cyber Systems. The language in bullet 2 includes "low impact," which is not an applicable system for this requirement. Therefore the guidance goes beyond the scope of the standard. This guidance should also be edited to be consistent with the language of the standard's requirement.

No

We agree with the following EEI comments: BES Cyber Asset – CIP-002.5.1 Guidelines and Technical Basis The definition of BES Cyber Asset combined with the guidance creates opportunities for misinterpretation. The scope of the reliability standards under Section 215 of the Federal Power Act is limited to "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability." (emphasis added) The BES Cyber Asset definition says "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which , if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System." (emphasis added) The Guidelines and Technical Basis section of CIP-002-5.1 (guidance) goes to some length discussing the concept of BES Reliability Operating Services (ROS) as a tool to identify the BES Cyber Systems that would be in scope. What "affect" means is made unclear by this guidance. If we arbitrarily assume that "affect" means "unable to perform one or more BES ROS" then the loss of a programmable device which provides status and magnitude of breakers, current flows, etc. for "Monitoring and Control" and "Situational Awareness", would be considered to be affecting the BES, and it would begin to do so immediately upon such loss. However, these devices are not necessary to operate "an interconnected electric energy transmission network" or "to maintain transmission system reliability." Therefore, we do not think this is what the Standard Drafting Team intended, however clarification in the guidance, which aligns with the scope of a reliability standard is needed. Removable Media There is a consistency issue. The definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to; however, the definition for Removable Media is not. It can be implied that the definition refers to connection to applicable systems, but it is not clear. It would also be clearer to switch the order of the Removable Media and Cyber Assets in the last sentence. Suggested Revision: Change the definition of Removable Media to: "Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets."

Yes

We agree with the following EEI comments: EEI supports the removal of the identify, assess, and correct language due to the expectation that NERC will refine its compliance and enforcement process under the Reliability Assurance Initiative (RAI) to move away from a zero tolerance approach to compliance. We expect the new RAI to be finalized prior to final ballot to address the zero tolerance concerns that the identify, assess, and correct language intended to address.

Yes

No

not applicable

Yes

We agree with the following EEI comments: CIP-002-5.1, CIP-005-5 and CIP-008-5 were not opened for revisions, comments or ballot. These standards contain one or more items that need to be updated to maintain consistency with the CIP standards which were opened. There are also items which need to be addressed to provide clarity for implementation and auditability. We respectfully request that the Revisions Standard Drafting Team make these "conforming changes" and other changes to the three standards regardless of whether they are opened for any other revisions. Examples include: • CIP-002-5.1, CIP-005-5 and CIP-008-5 all, in section 5, reference effective dates. These all need to be updated to be consistent with the effective date of the standards which

were opened for revision. • CIP-005-5 and CIP-008-5, in section 6, reference CIP-003-5, CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5 and CIP-010-1 and CIP-011-1. These references need to be updated to reflect -6 and -2 as appropriate
Individual
Leonard Kula
Independent Electricity System Operator
Yes
The IESO agrees in general with the requirement approach. We do not believe this will affect the IESO as our assets will be considered High Impact.
Yes
The IESO agrees with the requirement approach.
Yes
The IESO agrees with the requirement approach.
Yes
The IESO agrees with the revised definitions.
Yes
The SWG agrees with the requirement approach.
Yes
The SWG agrees with the requirement approach.
No
The IESO is not aware of any provincial or other regulatory requirements that need to be considered at this time.
No
Individual
James Gower
Entergy
No
CIP-003 R2 Part 2.3.2 requires entities to implement one or more processes that include “For Control Centers with external routable protocol paths, monitoring physical access point(s)” for Low Impact BES Cyber Systems. Executing this requirement would require entities to identify physical access points to Low Impact BES Cyber Systems which, in essence, would require the identification of a Physical Security Perimeter. This was not required under CIP-006-5 for Low Impact BES Cyber Systems. The risk reduction this requirement would bring is low due to the impact designation of Control Centers, where entities would protect all of the BES cyber systems located at and associated with the operation of those Control Centers designated as either High or Medium impact.
Yes
These changes are in line with the “ORDER REMANDING PROPOSED INTERPRETATION OF RELIABILITY STANDARD CIP-006-4” issued by FERC 3/21/2013.
Yes
Yes
Yes
No
With multiple effective dates for different requirements and sub-requirements, confusion may arise and result in an increased risk of potential violations. Making all requirements effective on the same date, or grouping compliance date by High, Medium, and Low designations would make for a more consistent transition to CIP Version 5.
No

Yes
: The naming convention for the standards should be standardized to prevent confusion. There are “CIP Version 5” standards that contain requirements suffixed -5 and -1. If the proposed revisions are approved, there will be standards suffixed -2,-5,-6, and -1 if CIP-014 is included. This is contrary to the precedent set by previous versions of the standards. Version 4 only contained changes to CIP-002, but all requirements in that Version were updated to -4, even though they did not change. Now the suffix is being incremented only when requirements have changes made to them, resulting in multiple suffixes. Requirements should all be suffixed with the same number to easily identify the current set of enforceable requirements as a package.
Individual
Erica Esche
Southern Indiana Gas and Electric Company d/b/a Vectren Energy Delivery of Indiana
Individual
Silvia Parada Mitchell
NextEra Energy
No
Looking at this from a risk perspective, the probability that someone will enter into a NERC CIP facility with access control devices, cameras, on-site personnel, etc. and then try to tap into the wiring, as opposed to just entering into the PSP and utilizing the BES Cyber System is not logical. Thus, NextEra recommends the following changes to the CIP-006, Requirement R1, Part 1.10 and its measure: By adding a paragraph to the Requirements Section which states: To restrict physical access to such cabling and components, the Responsible Entity shall document and implement one or more of the following: - Secured with conduit; or - Secured with cable trays; or - Implement alternative physical security control measures that utilize a defense in depth strategy that may include, but are not limited to: o multiple physical access control layers within a non-public, controlled space; o 24 x 7 security or operational personnel; o camera/video coverage; o other alarm systems; o multi-factor authentication devices; o other related security devices; Then under the Measures Section, modify the verbiage slightly to read: An example of evidence may include, but is not limited to, records of the Responsible Entity’s implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays or alternative physical security control measures) encryption, monitoring, or equally effective logical protections.
Group
MRO NERC Standards Review Forum
Joe DePoorter
Yes
Yes
Yes
The NSRF recommends that CIP-002-5.1 be updated (containing red lined and final versions) with the new and revised definitions.
Yes

: The NSRF supports the removal of IAC language from this fleet of Standards. We do not want any type of internal control or management practice to be an auditable instrument. Every entity needs to determine how they assess if they are compliant with EVERY applicable Requirement that they are registered for.
Yes
Unknown
No
Individual
Dan Roethemeyer
Dynegy
No
The Low BES Cyber Systems in the Applicable Systems column of the Tables would seemingly require a detail inventory similar to that required by Highs and Mediums to determine what are BES Cyber Systems. This should not be required per the Standard. If this is not what is intende then please provide guidance in the Standard as to how to determine Low Impact BES Cyber Systems without the using the detail inventory process.
Yes
Yes
On June 19, 2014, NERC gave a webinar on V5 and their was good Q&A at the end of the call. I thought their were many good questions but also many good answers that seemed to make sense from NERC. I couldn't write fast enough to get them down and repeat here but I suggest you get the recording (if available) and weave those answers into the Standards for guidance.
Individual
Kathryn Zancanella
South Feather Power Project
Yes
Yes
Yes
Yes
Yes
Part 2.6 of CIP-003-6 requires a quarterly "security awareness" component for entities with low impact cyber assets. For a small entity with few assets to begin with, instituting a quarterly "security awareness" communication could result in the opposite effect of what is desired. Rather than highlighting security awareness, such as is done during annual training that is already required by

FERC for hydropower licensees, a quarterly communication will take on the nature of routineness. I recommend changing Part 2.6 to require annual secuirty awareness communications.
Group
Arkansas Electric Cooperative Corporation
Philip Huff
No
We appreciate the approach to provide more specificity by using existing language from the other CIP Cyber Security Standards, and we support the language for all but the physical security Requirement Part 2.2. The requirement to restrict physical access does not provide sufficient criteria for entities to know they have satisfied the obligation. We suggest keeping the language of the requirement part and adding guidance to restrict physical access for BES Cyber Systems at a generation Facility and BES Cyber Systems at a substation. In particular, the guidance should confirm an approach whereby BES Cyber System components in a control house or control room can have greater physical protection applied than components distributed throughout the facility.
Yes
Yes
Yes
Yes
No
Overall, we feel the proposed timeframes are reasonable. However, we would like to submit a possible oversight in the timeframes for newly identified assets. There is currently no additional time given for newly identified assets with low impact BES Cyber Systems. It is possible for unplanned changes to result in an asset becoming part of the Bulk Electric System. In CIP-003-5, this was less of an issue because CIP-003-5 R2 was more programmatic and entities could address new assets as part of their overall program. The proposed CIP-003-6 R2 now has specific criteria, which necessitates consideration in the implementation plan for unplanned changes resulting in low impact categorization. We suggest a 12 month period for compliance implementation in this scenario. Also, we wish to express our support for the SDT completing all four Order 761 directive areas. It is important to have industry-developed objective criteria for the low-impact BES Cyber Systems when the requirements goes into effect on April 1, 2017. The industry begins its 7th year in which these Standards have been in development. It is difficult to grow and mature security programs with so much change in the compliance rules. We hope the industry, NERC and FERC can come to an agreement in the coming months and provide finality to these Reliability Standards for a time.
No
No
Individual
Michael Haff
Seminole Electric Cooperative, Inc.
Individual
Jo-Anne Ross
Manitoba Hydro
Yes
In Section C: Compliance Section 1.3, the meaning of “Complaints Text” is unclear
Yes
Yes

Yes
Yes
Yes
No
Yes
1) Given that the CIP standards become effective after governmental authority approval for most Canadian utilities, the CIP-002-5.1 and CIP-005-5 effective dates will be lagging behind the rest of revised standards by virtue of keeping CIP-002-5.1 and CIP-005-5 effective dates unchanged. We suggest changing the CIP-002-5.1 and CIP-005-5 effective dates to match the new implementation plan accordingly. 2) Under Section C 1.1 Compliance Monitoring, the CEA definition from a Manitoba Hydro perspective is incorrect as the Public Utility Board (PUB) is Manitoba Hydro's CEA. We suggest revising the definition to take Canadian utilities situation into account
Group
Colorado Springs Utilities
Shannon Fair
No
The Requirements proposed in 2.1, 2.2 and 2.3 are sound and apportion appropriate controls for Low Impact Cyber Systems. However, the "external routable protocol paths" language in Requirement 2.4 requires entities Low Impact Cyber Systems to provide and comply with "some form of electronic security perimeter," regardless of risk to the Bulk Power System/Bulk Electric System. Compliance to this requirement would be excessive given the risk associated with Low Impact rated BES Cyber Systems, and would require entities to maintain a list of Low Impact Cyber Systems, even though specifically not required by the standard.
Yes
Yes
Yes
Yes
No
Recommend changing the Implementation Plan time schedule to fall after the CIP Version 5 standards implementation dates. Entities are currently in transition from CIP version 3 to Version 5, implementing physical security controls, developing and enhancing policies, procedures, and security controls, preparing for audits, as well as performing the day-to-day operations of the systems.
No
CSU is not aware of any additional Canadian regulatory requirements that need to be considered during this project.
No
Individual
Patrick Farrell
Southern California Edison Company
Yes
Yes

SCE encourages the SDT to clearly provide entities with the choice between the physical access restrictions and the alternative means of protection, such as encryption of data, monitoring of the status of the communication link, and other logical protections. As we have a large and varied system, we will need the clear flexibility to select the best method of the system and environment. The proposed draft seems to suggest that physical protection is the first and preferred method, which could force entities to establish criteria for determining when to default to the alternative methods, thus complicating compliance.
Yes
SCE believes that the SDT's approach is sound, but believes that the final implementation plan for the entirely new Requirement 4 should reflect the additional procedural and record-keeping burden associated with it.
Yes
Yes
We accept the SDT's decision to remove the Identify, Assess, and Correct language from the 17 requirements in which it appeared, but believe that NERC must work expeditiously to complete the Reliability Assurance Initiative project and secure FERC approval of the project. The high frequency security obligations included in the CIP Version 5 Reliability Standards require that NERC and the Regional Entities exercise the enforcement discretion called for in RAI aggressively.
Yes
Group
Tennessee Valley Authority
Brian Millard
No
The Registered Entity suggests the SDT use the existing applicability tables throughout the standards to apply controls to Low Impact assets rather than consolidating in CIP-003 R2. The SDT has stated that they ‘pulled language and concepts from CIP-004, CIP-005, CIP-006 and CIP-008 to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2’. The language and concepts that have been pulled into CIP-003-6 R2 do not belong in the CIP-003 standard. The Registered Entity suggests the drafting team maintain consistency with the applicability tables found throughout the CIP version 5 standards and keep similar concepts grouped by standard. The Registered Entity strongly encourages the SDT to add protections to Low Assets in the appropriate CIP standard using the applicability table that already exists within the standards. CIP-003-6 R2.1 should stay in CIP-003. CIP-003-6 R2.2 and R2.3 should be moved to CIP-006. CIP 003-6 R2.4 should be located in CIP-005. CIP-003-6 R2.5 should be located in CIP-008. CIP-003-6 R2.6 should be located in CIP-004. Regarding R2.4: The terms ‘external routable protocol paths’ and ‘identified access points’ are ambiguous and may lead to inconsistent application and auditor interpretation without clarification. The Registered Entity suggests glossary terms be created to provide consistent application of requirements. Regarding R2.5: Can one incident response plan encompass multiple facilities/BES Cyber Systems? Does testing of the plan mean that testing must occur for each facility?
No
A. Need clarification regarding minimum acceptable data encryption standard. B. Need clarification regarding maximum acceptable opening size for conduit to be considered ‘secure’. C. For cable enclosed in conduit that spans a locked room between PSPs, what physical access controls should be applied to the room?
No
Regarding R4.5, need clarification regarding timeliness of signature / pattern files. How frequently does this update need to occur? Regarding R4.7, need clarification regarding minimum acceptable patching / mitigation prior to use. As written, creation of a dated mitigation plan appears to satisfy this requirement. There is no stipulation that mitigation must be completed prior to use of the asset.

No
Need clarification on what is meant by ‘directly connected’. Does it include specific media types (e.g. RS232, routable protocols, USBs, etc.)?
No
The removal of IAC from the standards requires that the RAI process be clarified regarding reporting timeframe and definition of ‘minimal risk’.
No
Effective dates should be reset to start with the approval date of CIP version 6. For large registered entities the level of effort to implement the standards on ‘Low Impact’ systems may now be greater than the burden of transitioning from version 3 to version 5 ‘High Impact’ and ‘Medium Impact’ systems.
<none>
No
Need clarification for what defines the lower threshold of the ‘Low Impact’ categorization. Does the BES definition serve to establish the lower boundary of the scope of the CIP standards?
Individual
Mikhail Falkovich
PSEG
No
The requirement for the ‘Low Impact’ security awareness goes above and beyond the equivalent requirement for High and Medium assets. We recommend removing the extra language in table R2 part 2.6 “Once every 15 calendar months, the program shall reinforce Parts 2.2., 2.3,2.4, and 2.5 above”. This will bring the language more in line with the equivalent requirement in CIP-004 R1.1. Additionally, we urge the SDT to reconsider the ‘quarterly’ periodicity of the security awareness reinforcement for Low Impact assets. While higher impact assets have a need for higher frequency of security awareness, the appropriate periodicity of reinforcement for Low Impact assets should be longer (annual periodicity is adequate).
Yes
Yes
Yes
No
While PSEG supports the approach of removing the IAC language and relying on the RAI function within NERC to manage the ‘zero defect’ issues, the RAI program has not yet been rolled out to the industry, and there is significant concern with the consistency of the RAI implementation. PSEG would like to have additional clarity and finalization of the RAI process prior to the implementation of the new standard language.
No
By the time this standard will be approved, the requirements impacting the low impact assets will change from the original CIPv5 requirements. Due to this fact, the industry should be allotted additional time to implement the necessary changes, as entities may have waited for finalization prior to initializing the low impact compliance/security projects. We request that the enforcement date for CIP-003-6 R2 be extended an additional 12 months to comply with CIPv6 low impact requirements.
No
No
Individual
Robert Ganley

Long Island Power Authority
Individual
Cliff Johnson
Consumers Energy Company
No
We agree with R2.1, R2.2, and R2.3. We do not agree with R2.4 as written. The Standard needs to clearly state that the access point can reside either at the substation OR at the remote end of an external routable protocol path. We do not agree with R2.5 as written. The language of the Standard needs to clarify that the Responsible Entity can create a holistic Incident Response plan utilizing physical security mechanisms that lead to Cyber Security Incident identification, classification, and response; and that logging and monitoring of Low Impact Cyber Systems is not required. We do not agree with R2.6 as written. The language of the Standard needs to clarify that the Responsibility Entity's security awareness program applies only to their employees, but could include non-employees, and that posters, emails, and topics at staff meetings are sufficient delivery method and that tracking of reception is not required. Overall comment, the Guidelines and Technical Basis contain the clarification language, but Responsible Entities are audited on the language of the Standard.
No
Comments: This has the potential to create significant undue burden on entities. The use of undefined terms such as "nonprogrammable" and "extended ESP" along with referencing between standards makes the requirement difficult to comply with. The sentence "In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP." From of the CIP-006-6 Guidelines and Technical Basis on page 37 leaves the requirement open to interpretation with no clear stopping point. The terms should be defined to limit the scope of the requirement and even though entities may utilize defense-in-depth controls beyond what is required, the requirement should be limited to the first termination point outside the PSP.
Yes
Yes
Yes
No
Not as written, but may be reasonable if adjusted according to entity feedback.
No
No
Individual
Candace Morakinyo
Wiscsonsin Electric Power Company (d/b/a We Energies)
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No

We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations. We Energies cannot vote to approve standards with "zero tolerance for exceptions".
No
We Energies is particularly concerned with Requirement R2.4 and its subrequirements, further explained in the Edison Electric Institute (EEI) response to question 1 on low impact requirements.
Not familiar with Canadian provincial or other regulatory requirements.
Yes
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations. Additionally, We Energies provides the following comments: * CIP-002-5.1 Attachment 1 Impact Rating Criteria 2.3 is not specific enough with respect to which BES Cyber Assets meet the criterion, or when they must be compliant. In general, it is understood that newly identified BES Cyber Assets must be compliant within one year of identification. However in this criterion, it is feasible that a generation Facility might be identified in a study looking out 5, 10 or more years with some level of uncertainty in study assumptions. Securing such a Facility is good business practice. Expending the effort to be auditably compliant years before the Facility actually becomes a limiting factor to BES reliability is wasteful of resources. Implementing compliance measures and incurring compliance risk is wasteful of resources if real world conditions change over time such that the Facility never becomes a limiting factor to BES reliability. * CIP-002-5.1, CIP-005-5 and CIP-008-5 all, in section 6, state that “An entity should include as much as it believes necessary in its documented process but it must address the applicable requirements.” It should also explicitly state that any entity-specific processes which go “above and beyond” the standard requirements will not incur regulatory compliance obligation. * CIP-003-6 Section 6 Background states that an entity should include as much as it believes necessary in its documented process but it must address the applicable requirements. It should also explicitly state that any entity-specific processes which go “above and beyond” the standard requirements will not incur regulatory compliance obligation.
Individual
Kayleigh Wilkerson
Lincoln Electric System
No
Although appreciative of the drafting team's efforts in developing the CIP Version 6 revisions, LES offers the following comments for the drafting team's consideration: CIP-003-6 R2.4.2 should be a sub bullet of 2.4.1. CIP-003-6 R2.5 – Requiring incident response on the Low Impact Assets seems unnecessary in consideration of the physical and electronic protections already required in the other draft CIP-003-6 requirements at the Low Impact Assets. Recommend the drafting team either remove R2.5 or else add an exclusion for ‘Low Impact assets without routable connectivity’ in recognition that a cyber-incident at a non-routable connected substation does not affect any other Low, Medium or High Impact BES Asset. CIP-003 R2.6 – Recommend the drafting team provide additional clarification regarding general awareness for Low Impact Assets. Is it the drafting team’s intent that awareness information be posted at every Low Impact Asset or is the posting of information in crew rooms and on intranet sites sufficient to meet this requirement? Additionally, do registered entities need to be concerned with contractors at their Low Impact Facilities and ensuring they get the quarterly awareness information too? In consideration that awareness training is already required of High and Medium Assets, LES recommends the drafting team consider, at a minimum, adding an exclusion to R2.6 for the ‘Low Impact assets without routable connectivity’ in recognition that a cyber-incident at a non-routable connected substation does not affect any other Low, Medium or High Impact BES Asset.

Individual
Michael Hill
Tacoma Public Utilities
No
Tacoma supports LPPC's comments on CIP-003 R2
Yes
One potentially unintended outcome of the wording of CIP-006 R1 [1.10] is a detailed cable map for each and every cable path relevant to an ESP in order to show protections for all of those that happen to fall within an ESP boundary, but not a PSP boundary. Detailed network diagrams may not be sufficient to prove whether or not a particular cable path falls inside, or outside a PSP.
No
Tacoma Power Supports LPPC's comments on CIP-010 R4 & CIP-004 R2. Additionally, Tacoma Power suggests CIP-010 R4 technical controls be moved to the like locations in CIP-007 (CIP-010 R4 [4.2-4.5] -> CIP-007 R3, CIP-010 R4 [4.7] -> CIP-007 R2). And move Authorization requirements to CIP-004 (CIP-010 R4 [4.1.1-4.1.2] -> CIP-004 R4) and Policy requirements to CIP-003 (CIP-010 R4 [4.1.3] -> CIP-003). Leaving CIP-010 R4 [4.1.4 & 4.6] in CIP-010, if they remain in the standard.
No
Offering a modification to the Removable Media definition below: "Removable Media: Media capable of removal without powering down the system, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media." This would remove the need to create a further definition of "Portable media." This definition would include hot-swop hard drives. Additionally, an argument can be made that all flash media contains a programmable microcontroller, and would therefore qualify as a Cyber Asset.
Yes
Tacoma Power Supports NERC's efforts to develop the Reliability Assurance Initiative (RAI) as a way to move away from a zero-tolerance enforcement approach.
Yes
No
No
Individual
David Rivera
New York Power Authority
No
NYPA recommends that the language added to CIP-003-6, table R2 (low Impact Assets) be moved to the specific tables in each of the Standards CIP-004-6 through CIP-011-2 where applicable. The inclusion of these control requirements with a unique table in CIP-003-6 result in Standards language inconsistencies that creates confusion and additional compliance risks. The following are some specific examples (not meant to be a complete list): A. A new definition is now needed (CIP-003-6 Rationale R2 and Part 2.4) for the phrase "external routable protocol paths" to ensure that entities and auditors clearly understand the differences between that phrase and the defined term External Routable Connectivity. This would avoid duplicating the confusion seen in earlier versions of the CIP Standards, such as the CIP-001 confusion between Facilities and facilities. The phrase "external routable protocol paths" may create a similar interpretation risk. B. With the new wording in CIP-003-6, table R2, security awareness (Part 2.6) is now more stringent for Low Cyber System than those that are High / Medium in CIP-004-6, R1 C. The Low Cyber System Incident Response Plan in Part 2.5, is very inconsistent with High / Medium Incident Response Plan required in CIP-008

R2 D. Policy requirements for Low Impact Cyber Systems would require a different set of policies to cover Low Cyber Systems for Entities with a combination of Low, Medium or High Cyber Systems. E. The shifting of the Low impact requirements to CIP-003-6, R2, breaks one of the prime objectives defined when CIP version 5 was being developed that each of the Standards (except CIP-002) be able to stand on its own. At entities with Low “and” either Medium or High Cyber systems, it would be necessary that CIP-003 “always” be referenced when any of the requirements in CIP-004-6 through CIP-011-2 are being designed and implemented, since dependencies are always possible between Cyber Systems part of any impact category. The end of result of having these Low Cyber System controls contained only in CIP-003-6, is that going forward, as the CIP requirements are refined and enhanced, the risk of new inconsistencies being created will always be a very higher. For example, if a slight change is made to a requirement in CIP-007-6, which somehow affects the set of Low Cyber Systems, then having to make a similar change to CIP-003-6, R2, in accounting for that change, may result in the change being missed or becoming inconsistent. These new set of CIP standards are already very complex, and any added confusion caused by this obvious structural problem will make it even more difficult (and costly) in meeting the Standards and likely negating the goal of improving overall reliability.
Yes
NYPA supports NPCC comments to this question.
Yes
Yes
Yes
No
NYPA Supports NPCC comments to this question.
No
Yes
NYPA Supports NPCC comments to this question.
Individual
Brenda Hampton
Luminant Energy Company, LLC
Yes
Luminant appreciates the work the drafting team has put into these standards. We agree with the general direction, but do have comments to provide clarification within the language. (1) For CIP-003, R2 the Rationale section states that “external routable protocol paths” is intended to focus only on paths to the low impact BES Cyber Systems rather that other networks such as Corporate. Can this be a defined term to explicitly state that rather than rely on the Rationale section? (2) CIP-003, R2.2 lists operational and procedural controls to restrict physical access. What is the difference between these two controls? Please provide examples. (3) The intent of CIP-003, R2.4.1 is dependent upon a definition of paths that can vary for each entity. The emphasis is needed on the controls that are implemented for clarity and measurable objective criteria. Please consider the following as a revision to R2.4.1: “Access points must be used to control routable communications to destinations and/or sources external to the BES asset where Low Impact BES Cyber Systems are located.” This revision places the emphasis on documenting the controls that accomplish the goal of restricting electronic access. (4) In Section C, part 1.3 the listed “Complaints Text” is confusing. Is the inclusion of the word “text” a typo? If not, please provide some context for this statement. (5) CIP-003 VSLs table can be challenging to follow. Consider removing redundant language wherever possible. Potential text edits include: (a) R2, item 1 “but failed to address one of the topics included in Requirement R2, Parts 2.2-2.6.” instead of referencing the text that references other texts (page 18 of 32). (b) R2 applies to low impact BES cyber systems. Is it necessary to repeat “with a low impact rating” or “for assets with a low impact rating” throughout the VSLs? (6) Suggested revision for CIP-003 “Guidelines and Technical Basis Section” Paragraph 2.2. This section includes a

statement of “operational or physical controls” however this language should match the requirement language which reads “operational or procedural controls”. (7) Suggested revision for CIP-003 “Guidelines and Technical Basis Section” Paragraph 2.3. (a) This section includes a statement of “external routable connectivity” however this language should match the requirement language which reads “external routable protocol paths”. (b) Since the primary purpose of monitoring is to watch for unauthorized access. Consider the revised language for the last two sentences: “Monitoring does not imply logging and maintaining logs, but monitoring that access has occurred at an access point (e.g., a door has been opened or traversed). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity’s controls.” (8) Suggested revision for CIP-003 “Guidelines and Technical Basis Section” Paragraph 2.4. (a) Within examples of sufficient access controls, the “public internet” seems to be a preferable listing rather than “world-wide-web” to include various external locations. (b) Within examples of sufficient access controls, details are provided for dialup modem connections. Is it the intent to not allow the modem to accept calls from authorized numbers? Should the wording be revised to clarify that calls from authorized numbers can be configured to autoanswer. Does the authorized phone number represent “some form of access control”? (c) Consider the following revisions to change the access technology to be more generic to not inadvertently restrict technology changes in the future. Consider revised language: “An asset has external routable connectivity due to a BES Cyber System within it having a wireless communications card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet on an unrestricted basis and from search engines such as Shodan.”
Yes
(1) The language in CIP-006, R1.10 seems to be in conflict with the Applicability section of CIP-007, R1.2. CIP-006, R1.10 includes only “nonprogrammable communication components outside a PSP” while CIP-007, R1.2 includes “nonprogrammable communication components located inside both a PSP and an ESP”. This conflict could be interpreted to imply that “entity owned and managed nonprogrammable network devices”, which are also “nonprogrammable communication components” are to be exempt from CIP-007 R1.2. Consider revising the Applicability section of CIP-007, R1.2 (which is not included in the current comment and ballot scope) to state the following: “Nonprogrammable communication components that are entity owned and/or managed and located inside an ESP.” (2) For the VRFs/VSLs for CIP-006-6, R1 and R2 please provide some understanding for removing all but Severe VSL. What would this mean if an entity has a process documented and implemented but fails follow it perfectly? For instance, what if an entity has a process to retaining logs for 90 days but unfortunately actually retain all the logs. Is this not a violation since it does not rise to the level of Severe?
No
(1) The wording for the Applicable Systems and the Requirements in CIP-010-2, R4 should be consistent to avoid potential confusion across the various parts of the requirement. Potential revision is to add “on applicable systems” to R4.1, R4.6, R4.7 and “prior to use on applicable systems” to R4.5 OR remove “on applicable systems” from R4.3. (2) CIP-010-2, R4.3 and R4.6 include the language “prior to use.” This language is problematic due to the ambiguity of “use” and leaves much to interpretation. There is language provided in the Guideline and Technical Basis, but enhanced language within the standard requirements would provide more clarity of the SDT intent to all industry segments. Additionally, it does not address Medium Impact BES Cyber Systems that are not required to be inside an ESP (or even a PSP) because they do not use routable protocols. Such devices are not subject to proposed requirement R4.6 but are subject to proposed requirement R4.3. (3) There appears to be a gap in CIP-010-2, R4.5. If an entity were to have a Transient Cyber Asset connected for 29 days, that Transient Cyber Asset should not necessarily have signature files that are 29 days old. Instead, if a Transient Cyber Asset is connected during a regularly scheduled signature update for non-transient devices, that Transient Cyber Asset should also be updated. The following language is suggested as an addition to the Requirement for R4.5 to remediate this gap: Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 when Transient Cyber Assets remain connected during regularly scheduled updates pursuant to CIP-007-Table R3 Part 3.3. (4) There appears to be a gap in the requirements if a PCA is used in any way other than it use as specified in R4.1.3. Consider the addition of CIP-010-2, R4.8 as follows to close this potential gap in the standards. If language is added, revisions are also needed in VRFs, VSLs and guidelines.

PART 4.8. APPLICABLE SYSTEMS: High Impact BES Cyber Systems and associated PCA, Medium Impact BES Cyber Systems at Control Centers and their associated PCA. REQUIREMENTS: Evaluate Transient Cyber Assets in accordance with 4.6 and 4.7 after any use not included in Part 4.1.3. When the evaluation results indicate the Transient Cyber Asset has been modified, take one of the following actions prior to use: -Remediate by returning the Transient Cyber Asset to the documented state in Part 4.1.4; or -Update the documented state in Part 4.1.4. MEASURES: An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities. (5) Guidelines and Technical Basis, Requirement 4. There is some good information included as a reference to support a clear understanding of the standards and requirements. The examples of transient devices that are provided could be strengthened with further specifying the intended meaning for Hardware/software diagnostic test and Hardware/software packet sniffers to clarify what the devices are used for. Possible revisions or additional language could include: ""Software diagnostic test equipment" is hardware equipment running such diagnostic software" and "Hardware/software packet sniffers" to "Hardware device running software packet sniffers. Which means an asset is categorized by a hardware component and specific associated applications or software they are running." Revisions to these bulleted items will improve the clarity and provide guidance to industry. (6) Guidelines and Technical Basis, Requirement 4, Parts 4.2, 4.3, 4.4 and 4.5. (a) The statement, "Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use" is reasonable, but the actual requirements do not make this clear. Revisions are needed to the appropriate requirements statements to clarify the SDT intent. (b) The statement, "For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use" has the same problem as Requirement 4.3: What is a "use" as intended for the standard? (c) A later paragraph states, "For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident." The second sentence seems ambiguous and could lead to different interpretations for entities and other stakeholders. How is an entity supposed to decide whether or not malware that is (1) detected and (2) removed before a transient device is connected qualifies as a Cyber Security Incident? It may or may not be easy to tell. Are entities expected to keep records of such occurrences? We suggest removal of the second sentence above and allow the entity to handle the malicious code detection within existing response requirements and avoid introducing this requirement here. (d) The next paragraph states, "Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns." The requirements in CIP-010 R4 do not require testing. This last sentence should be removed or revised to only include "process to document the installation of updated signatures or patterns." (7) Guidelines and Technical Basis, Requirement 4, Parts 4.6 and 4.7. The first paragraph states, "Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state." The term "prior to use" can be interpreted different ways (e.g. the start of a new workday, start of work within an ESP after leaving another ESP across the hall, start of the work week due to Transient Cyber Asset not being in direct control of the employee over the weekend, etc.) The "prior to use" language needs to be amended to avoid forcing entities to perform R4.6's specified tasks in situations when it is not required or needed.
Yes
Yes
Yes
No

Individual
Venona Greaff
Occidental Chemical Corporation
No
Occidental appreciates the work the SDT has done in response to FERC's directive in Order 791 to "address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets". However, we do not agree that the SDT developed objective criteria. Instead of establishing reasonable limits on the extent of evidence required to validate that an entity is providing sufficient physical protection, electronic access controls, cyber-incident preparation planning, and awareness training, R2 leaves the discretion up to the CEA. In order to prevent uneven application of the requirement across Regions – or changing over time – Occidental makes the following recommendations: 1) Change the focus of each sub-requirement from "implementing one or more processes" to "develop and maintain one or more processes". The 36 month recurring validation of the incident response plan (R2.5.6) would serve as a proxy for evidence of implementation – perhaps with an additional statement indicating that at least one Cyber System's physical/electrical protections must be evaluated as part of the exercise. Thus, the sample itself is under the entity's control – but the requirement could provide the minimum scope of cyber controls that must be validated. 2) Change the language in the Measures from "Examples of evidence may include, but are not limited to:" to "Each bullet point below provides an example of evidence sufficient to satisfy this requirement". A catchall bullet point would be needed to state that the entity is free to provide other equally effective evidence that satisfies the requirement. Although Occidental respects the good work that NERC has done to move away from zero-tolerance compliance methodologies, non-binding assurances that a reasonable compliance assessment will always be applied are not enough. Subjective interpretations by Regional Entities are still a very real concern. In the fast moving world of cyber security, it is far too easy to apply 20-20 hindsight to determine that an entity "should have been better prepared" for a new cyber-attack vector that did not exist when the protective strategies were developed.
Abstain
Abstain
Yes
No
In Order 791, FERC articulated that they understood the intent of the IAC language, but did not agree with the strategy taken to implement it. The Commission shared the concern that the rapid evolution of cyber-attack methods required flexibility in the protective strategies Responsible Entities deployed to address them. Forcing the industry to take mitigating steps to address future cyber-security incidents based upon the cyber environment in 2014 could be problematic. The SDT's approach in removing the IAC language and providing assurances that CEAs will apply appropriate consideration (via RAI process) for unknowable changes in the cyber-environment is somewhat concerning. Although OCCIDENTAL is a proponent of RAI and agrees that the regulatory community has taken positive steps in the direction of risk-based compliance, we have concerns that reason may not prevail in the aftermath of a destructive cyber incident. As mentioned in our comments to Question 1, subjective interpretations by Regional Entities are still a very real concern. Question 4 in the Identify, Assess, and Correct and Reliability Assurance Initiative FAQ document and its response reinforces our concern. How has the SDT chosen to address the concerns of IAC? The SDT discussed the concerns and options within FERC Order 791 and revised the 17 requirements containing IAC by removing the language. The approach fulfils the Order 791 directive regarding the IAC language and leaves resolution of "zero defect" or "zero tolerance" to the RAI 'discretionary path to enforcement' implementation. We appreciate the difficult task the SDT faced in addressing this issue because we too are hard pressed to come up with an equally effective method of addressing FERC's directive. We also recognize that delaying addressing FERC's directives with regard to IAC until RAI is officially rolled-out is problematic. But, until industry as a whole understands, and experiences first hand, a successful RAI approach, the requirements leave too much open to regulatory interpretation. The ancillary documents provide some guidance but in the end only the requirements within the Standards are subject to compliance and are enforceable. Our proposed alternative would be to encode the IAC concept into separate sub-requirements under each of the 17 affected requirements.

An example binding method might take the following form: Requirement Header: Each Responsible Entity shall implement a <program, procedure, policy> in a manner that is consistent with its best understanding of the cyber threat and protective strategies available at that time. A list must be included in the <program, procedure, policy> that captures the Responsible Entity's assumptions. Sub-Requirement A: At least once every 3 years, or after experiencing a Reportable Cyber Incident, or upon receipt of a NERC Alert related to this requirement, the Responsible Entity will perform and document an assessment of the adequacy of their <program, procedure, policy> and the assumptions. Sub-Requirement B: The Responsible Entity will develop and execute a Corrective Action Plan within 30 days of an adequacy assessment performed in accordance with Sub-Requirement A which indicates a reliability gap has been detected.
Yes
Abstain
No
Group
Dominion
Connie Lowe
No
Dominion suggests the SDT revise the wording of Part 2.1 to indicate "Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.". Without the word "applicable", a registered entity would have to have a policy associated with "Low Impact BES Cyber Systems at Control Centers" even if the entity doesn't have any "Low Impact BES Cyber Systems at Control Centers". Part 2.4.1 uses the term "external routable protocol paths". Clarity is needed to understand what "external" is in reference to. Provided there are no defined ESPs associated with Low Impact BES Cyber Systems, there are no defined external routable paths. Additionally, private network connections can exist between relays at different "impact rated" substations and restrictions should not exclude or preclude vendors from improving communications between relays by converting from a teltone connection to a digital connection. The requirement of defined access points and access permissions could interfere with such progress. Dominion believes that this requirement should be clarified to apply solely to external interactive access. Dominion suggests Part 2.6 should be revised to state: "Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months." As written, the requirement is more prescriptive than requirements for medium and high impact BES Cyber Systems. The language of the requirement should reflect the low impact rating of the asset class. Dominion notes that certain requirements, such as 2.3, may not apply to an entity, therefore, the language of the Part should not be overly prescriptive such that the concept of 'applicability' is excluded.
No
In general, Dominion agrees with the approach, but has concerns regarding how the last bullet in CIP-006-6, Requirement 1, Part 1.10 will be measured. The language of the last bullet states "• an equally effective logical protection". In order for this language to be auditable, a determination would have to be made on the effectiveness of the logical protection when compared to the first two bullets which state "• encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or" If an equally effective logical protection is required to be documented, Dominion believes clarification is needed regarding 1) how the protection would be measured and 2) who would be responsible for making the determination of the effectiveness of the control.
No
Dominion suggests adding a sub-part under CIP-010-5 Part 4.1 that allows entities to authorize classes or groups of Transient Cyber Assets. The suggested language is "4.1.x. Transient Cyber Assets, individually or by class or group of like assets;" Change CIP-010-2 Part 4.1.4 to be

consistent with CIP-010-2 Part 1.1.1. Part 1.1.1 states “Operating system(s) (including version) or firmware where no independent operating system exists”. Part 4.1.4 states “Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).” Recommended language for CIP-010-2 Part 4.1.4 is as follows: Operating system(s) or firmware where no independent operating system exists, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability). Dominion also suggests that additional language be added to the Guidance and Technical Basis section of this Standard to clarify what “per Cyber Asset capability” means. For example, Dominion needs clarity in understanding the extent to which an entity should go to determine the Cyber Asset capability; if the device doesn’t have a direct method of providing internal diagnostic and baseline information about the device itself, does this qualify the Transient Cyber Asset as not having “the Cyber Asset capability” to provide this information? Part 4.1: CHANGE: Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances TO: Authorize the usage of Transient Cyber Assets individually or by group prior to initial use, except for CIP Exceptional Circumstances Part 4.2 -- Clarity is needed regarding the “(per Cyber Asset Capability)” clause. Additional language should be added to the Guidelines and Technical Basis to describe the purpose of this clause. In practice, Dominion believes the clause means that when method(s) to deter, detect, or prevent malicious code can’t be technically implemented on a Transient Cyber Asset, procedural and policy controls are adequate. Additionally, where technical controls could theoretically be applied to deter, detect, or prevent malicious code on the Transient Cyber Asset, but the technical controls aren’t a recommended or approved configuration from the manufacturer of the Transient Cyber Asset, procedural and policy controls are adequate to meet this Part. Dominion is concerned that the “theoretical ability to implement a technical control per Cyber Asset capability” will be misinterpreted as requiring entities to adopt any and all technical controls per Cyber Asset capability regardless of operational feasibility. Part 4.6 -- Clarity is needed regarding the linkage of this Part to Part 4.1.4. Is an entity expected to reauthorize the baseline list of “Operating system(s) or firmware where no independent operating system exists, and intentionally installed software” for a Transient Cyber Asset when it’s changed as a result of executing Part 4.6. Dominion suggests no re-authorization is required since Part 4.1 states the authorization is required prior to initial use.
No
Dominion suggests combining the last sentence from BCA and PCA definitions and add it to the end of the proposed definition for Transient Cyber Asset to read as; A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Transient Cyber Asset is not a BES Cyber Asset or a Protected Cyber Asset. Dominion can’t comment further until clarity is provided on the phrase “programmable electronic device” and it’s applicability to the Bulk Electric System. Dominion believes this phrase unintentionally includes assets that would divert focus from the true intention of the standards.
No
Dominion is in support of the removal of the language as long as the removal is in conjunction with the adoption of an industry-approved RAI approach to ensure there’s relief from the administrative burden imposed by zero-tolerance. An alternative approach to RAI would be to address FERC’s concerns by modifying the individual Parts of each of the CIP Requirements.
Yes
No
No
Group
Southwest Power Pool Regional Entity
Bob Reynolds
Yes

While the SPP RE agrees that the explicit directives in FERC Order No. 791 have been met, the SPP RE has two concerns. First, the SPP RE disagrees with the premise in the Guidelines and Technical Basis section of the Standard that compliance can be demonstrated purely through presentation of the documented processes at audit. There is an expectation that the documented processes will be implemented by the Responsible Entity. In fact, the VSLs for R2 specifically refer to implementation (or failure thereof) of the documented processes. The compliance auditor is expected to evaluate whether or not the documented processes have been implemented and it is best left to auditor discretion how to accomplish that review. Rather than asserting that there should not be an expectation of verifying process implementation, as can be inferred by the paragraph in question, the guidelines would better serve the Responsible Entity by advising them to consider how they would demonstrate implementation and compliance with their documented processes. The guidelines should inform the Responsible Entity and the auditor what is expected to comply with the requirements and not how the requirements should be audited. The comment that the SDT strongly believes sampling is not necessary is inappropriate and should be removed. Second, the protection expectation for Low impact BES Cyber System is a weak, periphery control at best. Two critical protective controls are missing, especially with respect to a control center environment, and those are security patching and anti-malware protections. The entity does not necessarily have to perform the extensive testing expected of higher impacting BES Cyber Systems, but it is well known that somewhere around 90 percent of all successful cyber compromises could have been prevented with up-to-date patches and up-to-date, active anti-virus solutions. Given the likelihood of trusted network interconnectivity between control centers with Low impact BES Cyber Systems and control centers with higher impacting BES Cyber Systems, this critical shortcoming could be the key to a successful, widespread cyber attack.

Yes

The SPP RE agrees with the approach in general, however the SPP RE believes that in the instance where monitoring is the alternative process implemented in lieu of physical access protections, the alert needs to include a follow-up response that investigates the cause of the alert, regardless of the duration of the outage or communication interruption. Ignoring a momentary interruption could result in not detecting a splice, tap, or in-line compromise (similar to a key logger placed between the keyboard and the PC). Obviously, long-haul circuit protection, especially when the communication path includes commercial carriers (such as AT&T) or third-party providers, is best provided through the use of encryption. Within a building or for short runs between PSPs as might be found at a generating plant, an investigation response is quite feasible.

No

CIP-010-2, Part 4.2 could be construed as mandating anti-malware on a transient device. If read in this manner, it would preclude the use of a hardened laptop where the laptop is booted from a read-only CD and the hard drive-based operating system has been removed. Installing and maintaining anti-malware in this instance would be an unnecessary burden. The SPP RE recommends including a discussion of alternatives to the use of anti-malware in the Guidelines and Technical Basis section at a minimum. CIP-010-2, Part 4.5 needs to be strengthened by requiring the signature files to be updated and current prior to each use of the transient device, where anti-malware solutions are used. As written, a process that calls for an annual update of the signature files, while unreasonable, would satisfy the strict language of the requirement. CIP-010-2, Part 4.7 should require the transient system to be fully patched and not permit an alternative mitigation plan. Transient devices are not operationally critical and thus there is no risk-based reason they cannot be regularly patched. As the transient device does not continuously reside within an ESP, it cannot be guaranteed of being afforded the risk-mitigating protections enabled by the ESP requirements. Introducing a transient device into an ESP effectively bypasses most, if not all, periphery (ESP) protections. That can only be mitigated by eliminating risk on the transient device itself to the maximum extent possible. The SPP RE strongly recommends that the discussion of Transient Cyber Assets in the Guidelines and Technical Basis for CIP-010-2 be updated to more clearly state the expectation with respect to “prior to use.” As written, the guidelines suggest the Transient Cyber Asset does not have to be evaluated or otherwise prepared "prior to use" as long as it does not change ESPs or PSPs. That could be construed to allow the Transient Cyber Asset to be used outside of the PSP/ESP and not have to be re-evaluated as long as it was connected back into the same PSP/ESP it was last used in. The SPP RE believes the intent, while not clearly stated, is for the Transient Cyber Asset to be evaluated or otherwise prepared for use within a defined ESP prior to use in the ESP after being used

elsewhere. The SPP RE also suggests that a Transient Cyber Asset could be used consecutively in multiple PSPs/ESPs as long as the Transient Cyber Asset is not used outside of a PSP/ESP in the interim. For example, consider the laptop used to perform maintenance on substation relays. As long as the laptop is connected only to substation relays within PSPs/ESPs, and never to anything else in the interim, the laptop could be moved and used in multiple substations without having to prepare it for first use for each substation being visited. Similarly, a laptop used for maintenance or vulnerability assessments could move between the primary and backup control centers as long as it was never connected to a non-ESP network in the interim. Once the Transient Cyber Asset has been connected to a Cyber Asset or network outside of a CIP ESP, the Transient Cyber Asset must be reevaluated and prepared for "first use" before using it again within an ESP. This provision, as suggested by the SPP RE, should be tempered by the concept found in the Guidelines of having a separate Transient Cyber Asset for each BES Cyber System impact level due to the differing degrees of protection afforded to BES Cyber Systems and Protected Cyber Assets of different impact levels. The discussion of Part 4.5 in the Guidelines and Technical Basis section of CIP-010-2 states that process to update the signature or pattern includes testing the signatures or patterns in the same manner as CIP-007-7, requirement R3. The requirement to test is not included in Part 4.5.

No

The definitions of BES Cyber Asset and Protected Cyber Assets explicitly exclude a Transient Cyber Assets, which is problematic if the definition of Transient Cyber Asset is too permissive. The definition of Transient Cyber Asset is broad enough that a Responsible Entity could, theoretically, treat BES Cyber Assets or Protected Cyber Assets as transient devices by temporarily disconnecting them from the network every 30 days. The definition should be revised to state "A Cyber Asset directly connected to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset, expressly for a pre-approved, temporary purpose and disconnected immediately upon conclusion of the temporary need. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." Similar treatment should be given to Removable Media. In this instance, the expectation should be applied to removable media used for a temporary purpose, such as data transfer, and immediately removed upon completion of the temporary need. Portable media, such as an external hard drive, "permanently" connected to a Cyber Asset should not be considered Removable Media. To complete the distinction, the SPP RE suggests clarifying the term by referring throughout the definitions and standards to "Transient Removable Media."

No

The goal of the IAC language was to remove the expectation of 100% compliance within the standards. While the RAI program can address the handling of an issue of non-compliance through a number of enforcement options, the RAI program does not eliminate the now-restored 100% compliance expectation of the standard itself. There are a number of requirements where a less-than-100% performance expectation can be explicitly defined. For example, the change control and configuration management program is intended to prevent unauthorized changes from being implemented. A performance metric could be developed that allowed for an infrequent (frequency to be defined) occurrence as long as the entity's detective controls detected the unauthorized implementation activity within a to-be defined detection period (perhaps 24 hours) and the unauthorized change was promptly investigated. Other requirements, such as CIP-007-6, Requirement R4 (Security Event Monitoring that includes a logging component), could include a performance expectation stated in terms of percent availability over a defined period (e.g., 99.99% over a rolling 12-month period, which equates to a maximum allowable outage of approximately 53 minutes over the 12-month period). Adding performance metrics to the requirements themselves provides defined, measurable, and achievable goals and expectations and would eliminate, in many cases, the need to even refer the issue to enforcement for handling. RAI could continue to address the enforcement handling of any issues exceeding the allowable performance expectations.

No

The compliance date for CIP-006-6, Requirement R1, Part 1.10 refers exclusively to BES Cyber Systems. Under CIP Version 3, all Cyber Assets within an Electronic Security Perimeter had to reside within the PSP and were subject to the provisions now found in Part 1.10. The implementation plan for Part 1.10 should be consistent with the actual Version 3 expectation. In other words, the extended compliance period should only apply to new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not previously subject to CIP-006-3,

requirement R1.1 by virtue of being contained within a CIP Version 3 Electronic Security Perimeter. The incremental changes introduced in CIP-007-6, Requirement R1, Part 1.2 are sufficiently straightforward that an additional six months to comply is not warranted. The requirement only applies to controls centers, which greatly limits the scope and potential impact of the change. With the exception of perhaps CIP-010-2, Requirement R4, Parts 4.1 and 4.6 that require an inventory of operating systems, firmware, and intentionally installed software, there is no reason the provisions of CIP-010-2, Requirement R4 cannot be in place upon the overall effective date of CIP-010-2. The expectations of Parts 4.2, 4.3, 4.4, 4.5, and 4.7 are basic security practices that are good utility practices that should already be performed. This risk of introducing malware into the Electronic Security Perimeter is too high to grant nine additional months to comply with these basis security controls.
Yes
The implementation plan for CIP-004-6 allows for the later of April 1, 2016 or first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority. However, only three months is allowed if approval by a governmental authority is not required. This appears to be an inadvertent inconsistency in the implementation plan. Additionally, there have been a couple of errata changes to the Guidelines and Technical Basis section of CIP-002-5.1 that have been submitted to NERC by the SPP RE. Specifically; (1) the guidance for Criterion 2.13 should have stated: "Criterion 2.13 categorizes as medium impact *those BES Cyber Systems used by and at* BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1." and (2) the discussion of Criterion 2.8 should state "Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) *or* 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon)." These changes should be incorporated into CIP-002-5.1.
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
Group
SPP RTO
Lesley Bingham
Yes
No comments
Yes
There is a concern about the last bullet in CIP-006-6 R1.10. We do appreciate the flexibility the last bullet provides and how it allows for technological solutions which may not exist today. A Responsible Entity may believe that they have implemented an “equally effective” control, but if the Compliance Enforcement Authority disagrees, then that leads to a contentious audit and possible violations and fines for the Responsible Entity. Additional examples may help to guide the Compliance Enforcement Authority and help them seek reasonable solutions when auditing.
Yes
The section of CIP-004 which was amended was Requirement R2, not R1. An additional comment would be to remove the word “with” in the addition in Part 2.1.9.
Yes
We do appreciate the clarity that removing the IAC language will provide. There is a concern that we are being asked to approve standards based on a program that is currently under development. By the time that a Responsible Entity will see how RAI is applied in audit situations, these standards, with the IAC language removed, will long have been voted upon.
Yes

Consistency of effective dates is very important in a compliance situation. Although the extra time for these standards is appreciated, having 4 dates to manage (April 1, 2016; October 1 2016 for CIP-007-6 R1 Part 1.2; January 1, 2017 for CIP-006-6 R1 Part 1.10, CIP-010-2 R4, and April 1, 2017 for CIP-003-6 R2) is a concern. We would recommend that the six month window for CIP-007-6 R1 Part 1.2 be extended to a nine month window, reducing the number of dates and outlying requirements.
N/A
Yes
We would appreciate clarification on CIP-003-6 R2 Part 2.6. That requirement could be read to mandate two training sessions: a quarterly security awareness program and an additional training once every 15 calendar months to reinforce Parts 2.2, 2.3, 2.4, and 2.5 of CIP-003-6 Requirement 2.
Individual
Daniel Duff
Liberty Electric Power LLC
No
2.4.2, as written, would require the reason for granting access be part of the electronic access process. Suggest elilinating the phrase "including the reason for granting access", and adding 2.4.4 "maintain a record of the reason for granting access".
Yes
No
As writtine 010 R4 assumes the registered entity owns and operates the transient devices and removable media. In many cases contractors do so. The requirement should not force RE's to maintain contractor devices by patching them, nor should it force RE's to keep logs of contractor equipment. The requirement should only focus on scanning such devices prior to use.
Yes
No
The IAC language was needed to gain consensus on the V5 standards. The SDT approach was to simply remove this language without creating an alternitive to a zero tolerance standard. At a minimum, the VSLs and measures should be rewritten to allow for minor instances of errors. For example, instead of a single instance of failing to revoke access for a transfer, rewrite the requirement to requre a process that assures the access is revoked, with a low violation if the process fails to keep instances under 5% annually, or less than 2 in cases where there are small numbers of transfers each year.
Yes
Individual
Amy Casuscelli
Xcel Energy
No
Xcel Energy has several concerns as detailed below. The FERC directive requested objective criteria to be able to evaluate the efficiency of the protections of Low Impact facilities while the rationale and the inventory statements of the proposed Standard state “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” The breakout of Control Centers in R2.3 seems contradictory to both the direction of FERC and the language in the proposed Standard. FERC directed objective criteria, not the identification of specific Low Impact BES Cyber Systems or a tiered level of approach of differing Low Impact BES Cyber Systems. It is recommended that R2.3 be removed entirely or combine R2.3.1 and R2.3.2 under R2.2. We would like to see additional clarity that requirements related to Low Impact systems can

be satisfied at the same time as those for Medium/High. For example, the organization can have a single incident response plan, which does not need to be tested separately for a Low system if a test covered a Medium/High as per CIP-008. These compliance requirements better align with the subject matter of their Medium/High counterparts (CIP-004, -005, -006, -008) and should be moved there, rather than stay in a CIP program governance Standard where they may be overlooked. R2.4.1 and R2.4.2 state that “all external routable protocol paths, if any, must be through one or more identified access point(s)” and “For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.” Xcel Energy feels that by stating that an access point is required for network connected low impact assets, the actual scope of CIP controls significantly increases for these sites. A utility cannot arbitrarily install an access point without performing additional CIP program controls that typically support an effective access point. This would include performing a complete inventory of all assets and their connectivity, developing and establishing ESP diagrams, and performing a vulnerability assessment to verify any potential needs for additional access points. Additionally, it would require periodic controls to validate the access point including equipment inventory, configuration and ESP verifications, as well as the performance of periodic vulnerability assessments to ensure the access point is effective. By stating that an access point is required, this in effect forces entities to implement the full program of CIP controls at assets identified as having a zero to minimal impact to the BES. As worded, the scope of this requirement would be an additional 150 substations for Xcel Energy, dispersed across multiple states. In order to meet the access point requirement, full CIP controls would need to be implemented with no additional protection to the BES. This would result in a 245% increase to the number of substations where controls would need to be implemented; the cost and time of implementation does not seem commensurate with the protection added. R2.4.3 requires “Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.” Xcel Energy is concerned with the scope expansion resulting from this requirement, specifically for assets that have little to no impact to the BES (Low Impact). Xcel Energy anticipates approximately 60 to 70 substations to be classified as medium impact substations under current CIP version 5 requirements. The proposed authentication requirement for dial-up connected low-impact assets would bring approximately 400 additional substations into scope. Identifying, implementing and maintaining configuration management and capabilities to ensure authentication functionality is maintained at an additional 400 substations across multiple states would be an immense effort that would have adverse impacts to utilities such as Xcel Energy. It may also deter operational capabilities as an entity could decide disconnecting dial-up communication would be a better business decision when compared to the expense and level of effort necessary to meet this requirement for low impact assets. R2.6 is much more prescriptive regarding content for the awareness program than CIP-004 R1.1 requirements for Med/High. It should be written more generally to not require specific topics. Additionally, the training and awareness frequency requirements for Low Control level assets are excessive. For example, the quarterly awareness training interval is the same as that required for Medium/High assets. This undermines the meaning of risk level and only serves to promote complacency or a tendency to ignore quarterly missives, rather than promote awareness appropriate to risk level. Because low category assets indeed have a low risk of grid disruption if compromised or lost, the training interval should be less than that of Medium or High Control level assets, to be commensurate with that risk. Xcel Energy fully appreciates that cyber threats are continuously evolving. However, we have incident alert and event management systems to provide notice and awareness of evolving threats to low level asset holders. The incident management process serves to provide awareness of emerging threats, if needed. This quarterly training interval exceeds that of many other very important grid management activities, such as node balancing, Emergency Operations Management, non CIP control center operations, etc. If these very important grid reliability activities do not require quarterly awareness reinforcement, yet have shown through operational history to operate reliably, why should CIP training be more frequent? R2.6 should be revised as follows: “Implement a security awareness program that reinforces cyber security practices at least annually. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4 and 2.5 above.”

No

Both the Standard and the RSAW use the wording “or an equally effective logical protection: but do not offer criteria on who or what would determine what constitutes “effective.” While we appreciate the attempt for flexibility, part of the FERC directive was to reduce ambiguity and provide concise direction for both the Registered Entity and the CEA; this vague definition does not seem to afford

that direction. We recommend either clarifying the words “logical protection” by replacing them with a level of encryption, use or armored wire, or by removing the third bullet entirely.
Yes
There is a huge dependency on RAI accomplishing the intent to remove “zero tolerance” elements of the standards.
Yes
No
No
Group
Edison Electric Institute
Melanie Seader
No
Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. ***4. Applicability*** The scope of dispersed generation in the CIP-003-6 Applicability section should be limited and similar to PRC-005. {Suggested Revision} Under the Introduction section, 4 Applicability, 4.2 Facilities, add the following statement after 4.2.2 All BES Facilities: “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back the reference to CIP-002-5 Requirement R1.3 in CIP-003-6 R2. ***6. Background*** With the addition of the table to Requirement R2, the Background Section should include a paragraph referencing the tables and the “Applicable Systems” Column to be consistent with the Background section of the other CIP standards with similar tables. {Suggested Revision} Add the following paragraph after the first sentence of the CIP-003-6 Background Section 6: “Requirement R2 opens with, ‘Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets.’ The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.” Also, add a paragraph similar to the “‘Applicable Systems’ Columns in Tables:” from other CIP standards into the Background Section 6 for CIP-003-6 for Requirement R2. ***Requirement R2*** Add back the reference to “for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3” to properly set the scope. Also, change the table reference to “CIP-003-6 Policies, Processes, Plans and Programs.” to match the proposed revision to the table title. {Suggested Revision} Change R2 to: “Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.” ***Table Title for Requirement R2*** The Table title for Requirement R2 “CIP-003-6 Table R2 – Low Impact Assets” does not match the format of the tables used in the other CIP standards, which focus on the requirements not the applicable systems. {Suggested Revision} Change the R2 table title to: “CIP-003-6 Table R2 – Low Impact Asset Policies, Processes, Plans, and Programs” ***Requirement R2, Part 2.1*** An entity may not have a low impact BES Cyber System at a Control Center (R2.3) and therefore R2, Part 2.3 is not applicable. {Suggested Revision} Edit text to read “that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 -2.6.” ***Requirement R2, Subpart 2.4.1*** Clarify that an external routable protocol path is “external” to the asset identified in CIP-002-5.1 R Requirement R1, Part 1.3 containing low impact BES Cyber Systems. {Suggested

Revision} Insert " bi-directional" prior to " external " and insert "to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems" such that 2.4.1 becomes: "All bi-directional external routable protocol paths to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems, if any, must be through one or more identified access point(s)." ***Requirement R2, Subpart 2.4.2*** Remove "by default" as it implies the use of a firewall, which limits access control options. For example, an entity could use access control lists on a router or switch to provide security for traffic control. However, routers and switches do not do this by default. This will allow entities more options on how to accomplish traffic control. Also, include a statement to allow documentation of access permissions individually or by group to provide more contrast to CIP-005-5 Requirement R1, Part 1.3 for high and medium impact BES Cyber Systems. Documentation for low impact assets individually or by group is consistent with the measure, but should be added to the requirement. {Suggested Revision} Remove "by default" and add "and document access permission reasons individually or by group" such that 2.4.2 becomes: "For each identified access point, if any, require inbound and outbound access permissions, deny all other access, and document access permission reasons individually or by group." ***Requirement R2, Part 2.6*** The specificity of what must be covered and having to track two time periods is more prescriptive than the requirements for medium and high impact BES Cyber Systems. The proposed revision uses language from the medium/high impact requirement (CIP-004-R1.1) with the time period adjusted to once every 15 calendar months to differentiate for the lower risk. Cyber security awareness can be addressed during annual training for employees and contractors in addition to other ongoing cyber security awareness communications. {Suggested Revision} Remove the references to the subpart requirements as they may not apply to all entities and remove the quarterly requirement such that Part 2.6 becomes: "Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months." ***Guidelines and Technical Basis*** Align the drawings and wording in the guidelines and technical basis with the requirement language.

Yes

Guidelines and Technical Basis Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity's control.

No

Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. ***Requirement R4, Part 4.1*** EEI members are concerned with unnecessary administrative burdens created by Part 4.1. For example, Authorization generally applies to users. A user of a Transient Cyber Asset should be authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. {Suggested Revision} EEI does not have a specific revision to suggest to address these concerns; however, we recommend a careful review of the specific concerns and suggestions raised by Registered Entities to help reduce the administrative burden of this part. ***Requirement R4, Part 4.7*** The requirement should be tied together better such that it clearly allows mitigation instead of patching, when justified. {Suggested Revision} Condense the language into one sentence to help clarify the requirement. For example: "Evaluate Transient Cyber Assets, within 35 calendar days prior to use, for applicable security patches and take one of the following actions: (1) apply the applicable patches, or (2)create a dated mitigation plan, or (3) Revise an existing mitigation plan." ***Guidelines and Technical Basis *** The Part 4.1 guidance conflicts with the "Applicable Systems". The guidance says the requirement (R4) "applies to any transient devices", yet the "applicable systems" in the requirements tables are not the transient devices. {Suggested Revision} Edit the language under Requirement R4 to: "This Requirement applies to Transient Cyber Assets and Removable Media that will be connected temporarily to an applicable system. Examples of these hardware/software devices include, but are not limited to: - Diagnostic test equipment - Packet sniffers - Devices used for BES Cyber System

maintenance - Devices uses for BES Cyber System configuration - Devices used to perform vulnerability assessments" The guidance for Requirement Part 4.1, says "Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets." Requirement R4, Part 4.1 says "Authorize the usage of Transient Cyber Assets ***prior to initial use***, except for CIP Exceptional Circumstances." (emphasis added) The guidance language should be edited to be consistent with the standard's requirement. Bullet 2, under Requirement Part 4.1, says "It may be reasonable to have separate Transient Cyber Assets for each impact level." Requirement R4, Part 4.1 is focused on High and Medium Impact BES Cyber Systems, not all BES Cyber Systems. The language in bullet 2 includes "low impact," which is not an applicable system for this requirement. Therefore the guidance goes beyond the scope of the standard. This guidance should also be edited to be consistent with the language of the standard's requirement.

No

Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. ***BES Cyber Asset – CIP-002.5.1 Guidelines and Technical Basis*** The definition of BES Cyber Asset is inaccurately quoted on p.17 of the Guidelines and Technical Basis section of CIP-002-5.1 (guidance), which creates opportunities for confusion and misinterpretation. A BES Cyber Asset is a "Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which , if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System." By contrast, p.17 of the guidance inaccurately quotes the final phrase of the BES Cyber Asset definition as follows: "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact [sic] the reliable operation of the BES." This mistake in the guidance introduces an unfortunate source of potential confusion about this important definition. This error should be corrected. {Suggested Revision} In guidelines, p.17, under heading "CIP-002-5.1," replace second sentence with the following: "The Glossary defines a BES Cyber System as '[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.' The term BES Cyber Asset is defined as follows: "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems." Generally speaking, the definition of BES Cyber Asset encompasses those programmable electronic devices that could relatively quickly (within 15 minutes) have an adverse impact on BES Facilities, systems, or equipment (without regard for redundancy) which would, in turn, affect the reliable operation of the BES." ***Removable Media*** There is a consistency issue. The definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to; however, the definition for Removable Media is not. It can be implied that the definition refers to connection to applicable systems, but it is not clear. It would also be clearer to switch the order of the Removable Media and Cyber Assets in the last sentence. {Suggested Revision} Change the definition of Removable Media to: "Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets."

Yes

EEI supports the removal of the identify, asses, and correct language due to the expectation that NERC will refine its compliance and enforcement process under the Reliability Assurance Initiative (RAI) to move away from a zero tolerance approach to compliance. We expect the new RAI to be finalized prior to final ballot to address the zero tolerance concerns that the identify, assess, and correct language intended to address.

No

Whether the timeframes in the implementation plan are reasonable and appropriate depends upon how and when the other concerns in these comments are addressed. EEI answered no to this question due to the specific concerns described in these comments.

Yes
EEI greatly appreciates the work of the Standards Drafting Team and the NERC staff. We support the efforts to have a consolidated revision to cover both the date sensitive and other FERC directives in a single filing. CIP-002-5.1, CIP-005-5 and CIP-008-5 were not opened for revisions, comments or ballot. These standards contain one or more items that need to be updated to maintain consistency with the CIP standards which were opened. There are also items which need to be addressed to provide clarity for implementation and auditability. We respectfully request that the Revisions Standard Drafting Team make these “conforming changes” and other changes to the three standards regardless of whether they are opened for any other revisions. Examples include: (1) CIP-002-5.1, CIP-005-5 and CIP-008-5 all, in section 5, reference effective dates. These all need to be updated to be consistent with the effective date of the standards which were opened for revision. (2) CIP-005-5 and CIP-008-5, in section 6, reference CIP-003-5, CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5 and CIP-010-1 and CIP-011-1. These references need to be updated to reflect -6 and -2 as appropriate. Although the RSAWs are not included in the Standards Development ballot and comment process, they are an essential aspect of Compliance Monitoring functions related to the NERC Reliability Standards. When reviewing Reliability Standards, RSAWs are reviewed as a fundamental component of the end to end review process much like definitions. As a result, EEI members ask NERC and the Standards Drafting Team to collaborate on the RSAWs to identify how comments filed separately (i.e., the standards comments and RSAW comments) will be addressed to ensure the integrity of the CIP V5, V6 Standards. Specifically, the proposed RSAWs materially change the scope and intent of the standards because they (1) impose new obligations that exceed the requirements of the standards, (2) add unnecessary administrative burdens, and (3) are inconsistent. Please see EEI’s RSAW comments filed separately for additional detailed comments.
Group
Seattle City Light
Paul Haase
No
The term "portable" in "removable media" may add confusion. Suggest striking "portable" and replacing with "removable without powering down cyber system."
Yes
SCL supports the approach to use RAI concepts to take the place of IAC language.
Yes
For consistency across Standards, Seattle supports a change in presentation of controls for LOW-ranked facilities and systems. LPPC and Seattle prefer that the controls for Lows be removed from CIP-003 and moved to the appropriate Part of each applicable Standard (i.e., Awareness activities for LOWs should be found with other Awareness activities in CIP-004-6, Incident Plan controls for LOWs should be found with other Incident Plan controls in CIP-008-6, and so forth). However, Seattle is aware of the substantive additional tracking burden this approach will place on small entities having only LOW-ranked facilities and system, and suggests the following alternative: 1) revised Standards as above, to include all activities for LOW-ranked facilities and system in their appropriate parent Standard. 2) Change the applicability section of these Standards (CIP-003 to CIP-011) to be applicable ONLY to registered entities with ONE or MORE facilities/systems ranked HIGH or MEDIUM through application of CIP-002-5. 3) add a new Standard CIP-012-1 that is applicable ONLY to entities with NO HIGH OR MEDIUM facilities/systems identified through application of CIP-002-5. This Standard simply collects all requirements/controls for LOWs in one place. In no case will requirements/controls for LOWs identified in new CIP-012-1 differ from those in CIP-003 to CIP-011; CIP-012 is intended as a solution that makes clear the obligations for LOW-only entities. Finally, if a new CIP-012-1 Standard is deemed impractical, Seattle strongly recommends that NERC develop an administrative solution that will very clearly identify the

obligations for LOW-only entities, perhaps by maintaining a list or spreadsheet that is kept with the CIP Standards.
Individual
Stacy Bresler
Individual
Individual
Si Truc PHAN
TransEnergie Hydro-Quebec
Individual
Mike Marshall
Idaho Power
No
CIP-003 R2.1 to R2.6: The applicability section of all these requirement parts addresses Low Impact BES Cyber Systems. It is counterintuitive to think that a list of Low Impact BES Cyber System will not be required to show compliance. CIP-002 also explicitly states that a list of Low Impact BES Cyber Systems is not required. This creates increasingly burdensome administrative work on the registered entities. The requirements for the Low Impact Assets should be measureable but not require registered entities to produce a list of Low Impact BES Cyber Systems as it would be contrary to the CIP-002 wording. The wording of these parts should be adjusted to address the Low Impact Assets and not the Low Impact BES Cyber Systems. CIP-003 R2.4 greatly increases the scope of the Low Impact requirements. Registered entities will be required to implement “identified access point(s)” for Low Impact BES Cyber Systems of which registered entities are not required to maintain a list. This will essentially require registered entities to provide a list of all Low Impact BES Cyber Systems which is explicitly stated is not required in CIP-002. Except for the time frame requirement CIP-003 R2.5 mirrors the CIP-008 requirements. Wouldn’t it be more appropriate to word the CIP-008 parts to be more all encompassing rather than creating a new requirement and part that creates additional administrative burden on the registered entities? Incident response is often handled through similar processes regardless of the impact of the system and is then categorized as a part of the incident handling process. By creating separate requirement in CIP-003 and CIP-008 it will different incident response plans each with their own evidence or the same plan that complies with both requirements with duplicate documentation and effort to show compliance with two separate standards. CIP-003 R2.6 is very similar to CIP-004 R1.1 and should be incorporated into CIP-004 R1.1 rather than having to duplicate administrative effort to show compliance with two awareness programs.
No
No issue was noted with the requirement CIP-006 R1.10 as it is written. However, it does little to meet the directive that was given in Order 791 to “create a definition of communication networks and to develop new or modified” standards. Communication components are an important part of the reliability of the grid and a definition of what and how the regulators expect the registered entities to comply with protecting them and all their many potential configurations would be an important step towards better security.
Yes
Yes
No
It is concerning that the “Identify, Assess, and Correct” (IAC) language has been so quickly discarded when it was added to move the regulations away from a zero defect approach. The RAI project certainly has potential but is still in various pilot projects that have not yet born widespread benefits to the industry. There did not seem to be any project teams focused on attempting to reword the IAC language to rectify some of the issues that were voiced and now the industry, that approved the v5 standards with the understanding the IAC language would help to move the regulations away from a zero-defect approach, is left with no time frames or guarantees of what the

RAI will become or when it will be implemented. More work should be done see if there is a way to fix the IAC language prior to it be discarded.
Yes
No
No
Individual
Heather Laws
PNM Resources
No
General #1: Limit the scope of dispersed generation in the CIP-003-6 Applicability section, similar to PRC-005. In section 4.2.2 of the Introduction section, under 4. Applicability, 4.2 Facilities, add the following statement after 4.2.2 All BES Facilities, “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back the reference to CIP-002-5 Requirement R1.3 in CIP-003-6 R2. PNM agrees with the suggested revision posed by EEI. General #2: A number of the requirements are effectively duplicated language of existing CIP requirements. PNM strongly disagrees with the concept that Low Impact controls should be within one requirement. It begs the question why the SDT would not do the same for Medium and High, but the answer is obvious: it is not efficient. Low Impact requirements that are effectively duplicating existing requirements need to be removed and “Low Impact BCS” added to the impacted systems (applicability section) of the respective existing requirements. Having all the Low Impact controls under CIP-003-6 R2 make this requirement a “spaghetti” requirement that the SDT said would not be the updated version of the standards. Entities do not need to deal with the monitoring and enforcement implications of another “spaghetti” requirement if they should happen to have a potential violation of this requirement. R2.1: Update as an open-ended ‘pointer’ to other Low Impact requirements. Suggested alternative re-write: “Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in all enforceable CIP requirements applicable to Low-Impact BES Cyber Systems.” With such a rewrite, there’s also no reason this could not be changed to a separate CIP-003-6 R1.2 requirement. Rename R1 content to be R1.1, and include initial R1 language using the ‘starter’ language common in most other CIP requirements. R2.2: Does not identify the types of access restrictions required. Strictly speaking, a simple unlocked door still ‘restricts access’, even if it can be readily opened by turning the knob. Is this acceptable? PNM suggests that without clearer language or enforceable guidance, regional auditors will take their own initiative to self-interpret and be highly prescriptive in this regard as to what is ‘acceptable’. Entities will be at the whim of regional variances and auditor discretion. As implied above, adherence to the guidelines is not a reliable expectation to establish compliance assurance unless NERC can forthwith declare Guidance as an enforceable component of the standard. R2.3.1: Escorting where? It is only ever implied that a physical security perimeter of some sort must be established, and yet the only way to enforce and audit compliance with many of the R2 requirements is to physically create one. This sub-requirement also relies on the controls of R2.2, even though R2.2 states as allowing for operational or procedural control. Procedural controls alone cannot be reliably audited vis-à-vis R2.3.1 to ensure escorting. Regional auditors may necessarily force physical controls, regardless, as part of their ‘auditing approach’, undermining the allowances within the standard. The SDT will have pushed Low Impact BCS into Medium CIP-006-6 territory, effectively negating the very reason for writing the remaining separate physical security sub-requirements below. R2.3.2: in order to monitor physical access points they must be identified, which means that, again a physical construct must be defined to identify the access points into it, which means that the perimeter must be controlled at all other non-access locations, which means that the entire exercise of this requirement defaults back to operating effectively similar to CIP-006.

PNMRs concern is that regional auditors will be given significant latitude as to how they wish to interpret the 'effectiveness' of the controls, and thus by extension an entity's compliance with the requirement. • How does one prove that monitoring is continuously implemented, without having some form of logging? R2.4.1: Suggested alternative re-write: "The electronic access point(s) of all external routable protocol paths to Low Impact BES Cyber Systems, if any, must be identified." Access points are modified by identifying 'electronic'… otherwise, every routable connection in fact has a physical access point into the facility and it can be readily identified. R2.4.2: Suggested alternative re-write: "For each identified external routable protocol electronic access point, if any, require inbound and outbound access control rules, including the reason for allowing access, and deny all other access." The terms 'permissions' and 'granting' could also potentially imply expected authorization activities, which is not what this requirement is supposed to be overseeing. Unfortunately CIP 005-5 R1.3 suffers the same flaw, and should also be fixed. R2.4.3: Since some regional auditing entities do not understand the strict meaning of the words "authentication" and "authorization", what constitutes authentication in this case needs to be clearly prescribed (NEEDS NEW GLOSSARY DEFINITION). Perhaps a cross-reference to NIST Special Publication 800-63 would be appropriate, or at least a Guideline reference to it. R2.5: This is an unnecessary and duplicative requirement. There's no clear reason why Low Impact BCS cannot/should not be added to "Applicable Systems" within the CIP-008 standard in lieu of this sub-requirement. Update CIP-003-6 R2.1 to point to this standard. R2.6: This is an unnecessary and duplicative requirement. Again, just add Low Impact BCS to CIP-004-6 R1/R1.1 "Applicable Systems" in lieu of this sub-requirement, and update CIP-003-6 R2.1 to point to this standard. Ironically, this requirement even has additional specific and more-stringent reviews and documentation requirements (assurance of topical coverage annually) than are necessary for Medium and High BCS under CIP-004-6 R1/R1.1. The explanation recently provided by SDT personnel (at the 6/19/2014 SDT webinar) is appreciated, but it nonetheless continues to violate the new NERC standards design methodology.
Yes
Guidelines and Technical Basis Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity's control.
No
PNMR agrees with the comments posted by EEI.
No
PNMR agrees with the comments posted by EEI.
Yes
PNMR agrees with the comments posted by EEI.
Yes
No
Group
Bureau of Reclamation
Erika Doot
No
CIP-003-6 R2.4.2 - Reclamation suggests that the requirement should be clarified so that restrictive routing schemes are considered sufficient access permissions.
No
CIP-006-6 R1.10 - Reclamation suggests that the requirement should be clarified to account for situations where cabling outside the PSPs is located in the same facility as the separated PSPs and that facility provides physical access only to authorized personnel. For these cases where installation of conduit is not possible and installation of encryption is not technically feasible, it should be clarified that physical access controls to the facility can provide adequate protections and are compliant with the standard. Therefore, Reclamation suggests that the list of acceptable physical access restriction examples in the Measures be updated to include "facilities that provide physical

access only to authorized personnel” in addition to “cabling and components secured through conduit or secured cable trays.”
No
CIP-010-2 R4.1.4 – Reclamation suggests that the drafting team add a bullet to the Measures that allows “an automated scan of the Transient Cyber Asset” prior to use on the ESP network as evidence for satisfying this requirement. CIP-010-2 R4.6 - Reclamation suggests that the drafting team add a bullet to the Measures that allows “an automated scan of the Transient Cyber Asset” prior to use on the ESP network as evidence for satisfying this requirement. CIP-010-2 R4.7 - Reclamation suggests that the drafting team add a bullet to the Measures that allows “an automated scan of the Transient Cyber Asset” prior to use on the ESP network as evidence for satisfying this requirement.
Yes
Yes
Yes
No
No
Individual
Thomas Breene
Wisconsin Public Service
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
No
These comments are submitted on behalf of the following PPL NERC Registered Affiliates: LG&E and KU Energy, LLC; PPL Electric Utilities Corporation; PPL EnergyPlus, LLC; PPL Generation, LLC; PPL Susquehanna, LLC; and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP. Comments: Would like to see the tie between CIP-002-5 R1.3 added back to the requirement, instead of just saying “containing low impact BES Cyber Systems”. Do not understand the removal of this tie in to CIP-002. For R2.4 shouldn’t the Applicable Systems section list “Low Impact BES Cyber Systems with external routable protocol paths Low Impact BES Cyber Systems with dial-up connectivity”, thus allowing Entities without those paths and/or connectivity, the option of not worrying about this requirement and just documenting the absence of the path and/or connectivity. For R2.6 revise the requirement to clarify the intent as follows: Implement a security awareness program that reinforces cyber security practices at least quarterly. At least once every 15 calendar months the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.
Yes
Including them in one place allows for concise understanding, however, a concern is that the auditors will look to the other requirements for measures or expectations of evidence. It needs to be clear, that while the requirement “mirrors” or is similar to one for High/Medium Impact Assets, the only option for audit and evidence resides within CIP-003 R2
No
Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity’s control.
No

No
Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity's control
Yes
We assume this applies to R2, part 2.1.9, since there is no R1, part 1.1.9.
Yes
Individual
Bill Fowler
City of Tallahassee, TAL
No
The City of Tallahassee (TAL) feels that Part 2.4 does not adequately illustrate the measures necessary to prove compliance to the part 2.4.2 requirement. The term 'representative sample' needs to be defined specifically. Does this imply a sample of rule sets from more than one access point? A sample of the rule set from a single access point? If more than one access point is identified, then would the entire rule set, or only a partial rule set from a single access point qualify as a representative sample? There can be no ambiguity when direct evidence is required as proof of compliance. Part 2.4.1 states that all external routable protocol paths, if any, must be through one or more identified access point(s). Evidence includes documentation of these paths through identified access points. If there is no requirement to discretely identify low impact BES Cyber Systems, then how can we be expected to provide evidence for this requirement when we are not required to identify the access point in the first place? External routable protocol paths imply the existence of an electronic security perimeter, a specific set of connected assets that form a basis for a defined network structure. There is no language in this requirement to identify an electronic perimeter, therefore no conceptual reason to identify an access point with routable protocol paths that may or may not be external to an undefined barrier. The language of this particular requirement and the measures required to prove compliance are extremely vague. Parts 2.1 – 2.3, and 2.5 are sufficient to address FERC Order No. 791 paragraphs 106-100, and clearly provide substantive objective criteria to sufficiently measure an entity's protection of low-to-no impact cyber assets. Requiring entities to identify assets (access points) where asset identification is clearly stated as unnecessary, and provide representative samples of configurations for these unidentified assets, assets that function as external access gateways to an undefined electronic security perimeter, could create an unnecessary quagmire of compliance effort. Under the section Guidelines and Technical Basis for part 2.4 it states that the Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. There is an assumption made here that at least one or more external routable protocol and/or Dialup connectivity paths exist and those access paths are being utilized to communicate directly with the asset from a remote location. This language should be rewritten to match the requirements in Part 2.4 – removing any unnecessary ambiguity with regard to direct communications pathways vs. other reasons for necessary connections via remote communications paths; e.g. "The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths, if any, to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected." Furthermore, the following sentence should be rewritten to state, "In cases where external connectivity is used to gain access to any low impact BES Cyber System at a remote site, electronic access controls should address the risk of using external connectivity." The final two sentences in this paragraph contain references to ambiguous concepts such as collection and aggregation, without stating specifically what kind of information might be collected and/or aggregated. TAL's contention is that these two sentences add nothing to the explanation and should be removed entirely. They state that these access controls are required to protect the collection and/or aggregation of low impact BES Cyber Systems, or the collection and/or aggregation of data pertaining to them, or what specifically?
Yes

No
Part 4.3 is identical to Part 4.2. I suggest collapsing 4.3 into 4.2 to include 'prior to use on applicable systems'. Both requirements are obviously meant to be done prior to use on applicable systems (intent of the standard in the first place), so there is no point in stating the same requirement twice. If the intent of this revision is meant to protect applicable systems, then the only requirement necessary is 4.3. If both requirements must stay, then remove the word 'detect' from 4.2 as detection is required prior to use as part of 4.3. It makes the most sense to collapse the two requirements into one and adjust the Measures language to include hardening policies and scanning techniques as part of the traditional antivirus … example.
Yes
No
I have no recommended alternative approach as I believe the original IAC language in the standard identified with a need to change industry perception of the spirit and intent of Critical Infrastructure Protection Reliability Standards to concentrate effective proactive compliance efforts towards identifying and correcting deficiencies rather than being focused on the fact that violations for those deficiencies may exist and subsequently turning the workplace into a reactive, audit documentation mill. The many changes in Violation Severity Levels in the revised standard will effectively result in potential violations regardless of any effort (or lack of effort) on the part of the entity to mitigate those violations. Now, with the IAC language removed, entities are no longer provided a much-needed greater degree of flexibility in detecting and remediating low-risk violations. All and any interpretation of the standards has been placed into the hands of auditors, which contributed to endless anxiety on the part of the entities with prior CIP versions. FERC stated concern over the broad and ambiguous nature of the IAC language as sufficient reason to force NERC to improve upon how the (IAC) language was written. As a result, NERC decided to assume that the enforcement process for low-risk violations would be unworkable, and remove the language altogether. This effectively disenfranchises the entity throughout the compliance auditing process.
No
Given the nature of the removal of the IAC language which results in a measurable change in how compliance programs would function under the new standard, FERC should issue an order to extend the effective date at least another full 6 months for each standard/requirement for which a modification to the language was made.
No
No
Individual
Megan Wagner
Westar Energy
Individual
David Jendras
Ameren
Individual
Ayesha Sabouba
Hydro One
No
Currently, all of the new requirements for addressing FERCs concerns about Low Impact BES Cyber Assets have been shoe horned into the Standard on Security Management Control even though many requirements mirror those covered in other Standards for High and Medium Impact assets. For instance, requirements related to physical access controls for Low Impact assets appear in CIP-003 whereas physical security requirements for other asset types appear in CIP-006. Requirements related to Incident Management for Low Impact assets appear in CIP-003 even though Incident Management for Medium and High Impact Assets is covered in CIP-008, and so on. This leads to a

needlessly confusing set of standards where reference needs to be made to multiple requirement statements in multiple standards simply to determine what needs to be done in a particular subject area. This increases the effort needed to implement the Standards, increases the effort needed to demonstrate compliance, is likely to lead to duplication of effort, and could increase the likelihood that Responsible Entities will overlook or misunderstand some requirements. Requirements for Low Impact assets that mirror requirements appearing in other Standards for High and/or Medium Impact assets should be moved to those other standards. 1. In the text of the first sentence of R2, delete the words “assets containing”. As the wording currently stands, all Low Impact BES Cyber Assets would have to be located within some sort of “container” (eg. a building or yard) and the protections stipulated by Requirements R2.1 through R2.6 would have to be applied to the entire container, not simply to the Low Impact Cyber Assets themselves. 2. For Requirement R2.4: a. Demonstrating auditable compliance with R2.4.1, R2.4.2, and R2.4.3 appears almost certain to require Responsible Entities to create and maintain inventories of Low Impact Cyber systems and their associated access points and permission sets, as well as an inventory of all Low Impact assets with dial-up connectivity. This is not consistent with the statement made in the “Rationale for Requirement R2” which states that, “creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome…..”. b. Requirement 2.4.1 refers to an “external” routable protocol path. External to what is unclear. The current wording could be read as “External to the Low Impact BES Cyber System concerned”, external to a Low Impact BES Cyber Asset, external to some (as yet unspecified) “electronic communications perimeter within which the Low Impact BES Cyber System resides”, or perhaps “external to the physical enclosure that “contains” the Low Impact BES Cyber Asset” (as implied by the unmodified text of R2). This needs to be clarified. c. As currently written, Requirement R2.4.2 applies in cases where communication with low impact assets is either routable or non-routable. This requirement provides little, if any, additional security if communications are not routable. d. Clarify whether or not the term “access point” in R2.4.2 includes places where one connects transient devices and/or removable media? 3. Modify the wording in the Table of Compliance Elements as follows: The High VSL for R2 should be revised to read, “…..but failed to address three or more of the topics as required by Requirement R2, Part 2.1 (2.1)…..”

Yes

Request CIP-007 R1 Part 1.2 Rational to be added to guidance and additional guidance provided. Suggest illustrative examples so that Entities and Auditors reach the same interpretation

Yes

1. In CIP-004 Requirement 2.1.9 delete the word “including”. Neither Transient Cyber Assets nor Removable Media are Cyber Assets. 2. In CIP-010: a. Requirement 4.1 refers to “Authorization” of usage, users, locations, acceptable use, and firmware/software. The Requirement should state clearly who it is that can provide this authorization. Possibilities include the CIP Senior Manager or Delegate, a person or group identified in the access management program pursuant to CIP-004 R4 (specifically R4.1), or the “individual or group with authority to authorize baseline changes as per Requirement CIP-010 R1.2. Recommend documented authorization as an option b. In Requirement 4.1.4 delete the word “intentionally”. Software that is installed unintentionally or illicitly should not be permitted unless it is known to be benign. c. In Requirement 4.1.4, reword Requirement 4.1.4 to read, “Operating system, firmware, installed software, including installed updates and patches, on Transient Cyber Assets (per Transient Cyber Asset Capability) d. Reword Requirement 4.3 to read “Use method(s) to detect malicious code on Removable Media and Transient Cyber Assets prior to their use on, or with, applicable systems” e. Reword R4.4 to state, “Remove or disable all malicious code detected on Transient Cyber Assets and Removable Media prior to use in, or with, Applicable Systems”. f. Reword the first portion of Requirement 4.6 to read, “Prior to use, and except under CIP Exceptional Circumstances, evaluate Transient Cyber Assets for modifications that deviate from the authorized configuration”. Reword the second portion of Requirement R4.6 to read, “for a modification that deviates from an authorized configuration, either; a) remediate by returning the Transient Cyber Asset to the most recently authorized configuration prior to use; or b) authorize the new configuration prior to use, including the parameters listed in Requirements 4.1.1 through 4.1.4 3. Reword to state that the transient cyber asset must not be interconnected between a higher security zone and a lower security zone – i.e. must not be “dual homed” 4. There need to be Requirements pertaining to the re-purposing and destruction of Transient Cyber Assets and Removable Media. This could be accomplished by expanding the scope of Applicable Systems in CIP-

011 R2 to include Transient Cyber Systems and Removable Media, or by mirroring the language of that set of Requirements.

Yes

1. The definition of “Transient Asset” should include devices which connect temporarily to EACMS (which are on, not “within”, the ESP) and/or PACS. This would provide a measure of configuration control and malware prevention to systems which are essential to the protection of BES Cyber Assets and their associated networks. For instance, without this protection a Transient Device with a legitimate connection at an ESP access point could, if compromised, jeopardize the effectiveness of the access control and/or the capability of networks or devices within the ESP.

Yes

No

Please provide a clear and consistent time line for implementation of these requirements. Ensure that all new effective and mandatory dates are after their CIP V5 dates. The current format is confusing.

No

Yes

Hydro One supports TFIST recommendations on NERC Project 2014-02 CIP Version 5 Revisions Standard. Drafting Team should be allowed to help clarify and provide guidance for industry issues and items discovered in the pilots. Hydro One also agrees that In particular the following should be addressed by NERC with the SDT representing industry: 1. Transfer Trip: CIP-002-5 R1, ‘transmission stations and substations’ for medium category assets, what some refer to as the “transfer trip” issue. 2. Clarify the term “programmable devices” which is an undefined term open to strongly differing viewpoints. 3. Clarify “effect within 15 minutes” issue and the burden of evidence for proving that something does not exist. Please clarify if diversity vs redundancy can be considered as part of the Entity’s impact assessment (i.e separate system using a different technology) Recommend adding “or” to CIP-010 R4 Part 4.1.4 to make this Part consistent with CIP-010 R1 Part1.1.1. Part 1.1.1 requires a baseline of Operating system(s) (including version) OR firmware where no independent operating system exists; while Part 4.1.4 requires Authorization to include Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability). Part 4.1.4 requires Authorization of both Operating System AND Firmware for a transient device while Part 1.1.1 requires baseline of Operating System OR firmware. We suggest the proper approach is to retain the OR. When applying R4 to a laptop we normally record the OS and version and not look to the firmware BIOS.

Individual

Steve Hamburg

Encari

No

Supporting Comments Requirement R1.2 pertains to a required policy for “Electronic Security Perimeters (CIP-005) including Interactive Remote Access” but the required implementation of that policy appears to have a broader scope in Requirement R2.4.1 which pertains to required processes for “All external routable protocol paths, if any, must be through one or more identified access point(s).” The latter requirement, R2.4.1, is not limited to interactive remote access that is the subject of R1.2. The Rationale for R2 explains the phrase “external routable protocol paths” is used instead of the defined term “External Routable Connectivity” because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term “External Routable Connectivity” in the context of Requirement R2 is not appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. Inconsistently, the Guidelines and Technical Basis section continues to use the term “external routable connectivity” in the discussion of R2 in the two statements below: “2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required.” 2.4 … “An asset has

external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan."
No
Supporting Comments The applicable scope of CIP-010-2 R4 is too narrow; it should be expanded to include the EACMS and PACS that are associated with High and Medium Impact BES Cyber Systems. EACMS and PACS need to use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability). The omission of EACMS and PACS from the scope of protection under CIP-010-2 R4 is inconsistent with the protections afforded to EACMS and PACS under CIP-007-6. CIP-007-6 Requirement 3.1 provides that High and Medium Impact BES Cyber Systems, and their associated EACMS, PACS, and PCA must deploy method(s) to deter, detect, or prevent malicious code.
Yes
Individual
Daniel Gibson
KCPL
No
R2 – Usage of the term "external routable protocol paths" should be officially defined by NERC before being able to "judge the sufficiency" of the newly introduced controls. Assumptions a responsible entity could make surrounding this term could lead to violations. The Guidelines and Technical Basis section includes numerous references to "belief" and "intent," along with descriptions of what entities "should" be doing. The need for such language indicates that the requirement language is not able to stand on its own and results in a need to be audited by the Guidelines and Technical Basis section. In turn, language not intended to be a required action by the entity could result in a perceived additional requirement by those trying to understand the requirement. While the intent of the "Note:" section under CIP-003-6 R2 is understood, there is no way to effectively audit for the successful and complete implementation of CIP-003-6 Table R2 – Low Impact Assets without obtaining an inventory of considered assets and of authorized users. Auditors are not able to reliably issue a judgment of the effectiveness of an internal control or of adherence to requirements without ensuring that samples are pulled from a complete population. Furthermore, entities are not able to perform the functions outlined within the R2 requirements without having lists of authorized users, both for access authentication and monitoring purposes. R2.3.2 – In part because the reference to "physical access point(s)" is not in relation to a defined Physical Security Perimeter, the requirement is actually more stringent than that of CIP-006-6 R1.4 and could require more evidence in support of compliance. An entity may need to prove an evaluation was performed resulting in the derivation of an inventory of all potential access points for all Low Impact BES Cyber Systems at Control Centers. Furthermore, diagrams may be needed to support that monitoring has been considered and defined for all applicable access points. While intended to be helpful in aggregating all Low Impact BES Cyber Systems requirements into a single section, the table has resulted in a web of functionally similar, yet separated requirements that could result in confusion. KCP&L recommends that, wherever possible, the items from CIP-003-6 Table R2 – Low Impact Assets be moved to the appropriate functional section and included as an additional applicable system where requirements are also similar. R2.4 – The requirements established under R2.4 are redundant to CIP-005-5 R1. In order to effectively audit the implementation of such controls, inventories and lists will be required just as they will be for CIP-005-5 R1. Guidelines and Technical Basis Section 2.4 – The two sentences beginning with "The electronic access controls should address…" go beyond the purview of the language of the requirement and serve to dictate what "should" be addressed. It is recommended that these sentences be stricken from the Guidelines and Technical Basis section.

No

CIP-006-6: The current order and applicability for CIP-006-6 is inconsistent and does not logically flow. At no point is a requirement for use of a defined PSP introduced, yet a number of the requirements pertain exclusively to the existence of a defined PSP. Physical Access Control Systems, as defined by the NERC Glossary of Terms, are also not stated as being required. Due to the current combined applicability and requirements, an entity could theoretically have a High Impact BES Cyber System that does not reside in a PSP and does not have a Physical Access Control System. This could result in applicability of only CIP-006-6 R1.3 and R1.10, and a lack of requirement for operational or procedural controls to restrict physical access. While the entity would still have to achieve two or more physical access controls, the requirements never state that a PACS is required for a High Impact BES Cyber System to achieve this or that a PSP is required for any system. KCP&L recommends that either CIP-006-6 R1.1 be updated to require the use of a Physical Access Control System for High Impact BES Cyber Systems or that a new sub-requirement is created to require High Impact BES Cyber Systems to have a Physical Access Control System with defined operational or procedural controls to restrict physical access. In addition, consideration should be given to rewording some monitoring, logging, and alerting requirements to include monitoring, logging, and alerting provisions for non-PSP, physically protected areas. CIP-007-6 The term “nonprogrammable communication components located inside both a PSP and an ESP” is a new source of confusion and may require definition as an official NERC Glossary term. CIP-005-5 requires only for “Cyber Assets” to reside within an ESP. Unofficial guidance has already been communicated by various Regional Entities in support of excluding non-Cyber Asset, nonprogrammable “devices” from the required ESP. Therefore, it is difficult to identify where a “nonprogrammable communication component” that is also not a Cyber Asset would be located inside an ESP. Additionally, while CIP-006-6 defines certain protections that must be afforded to a Physical Security Perimeter, there is no requirement stating that a device must reside within a defined PSP. Therefore, entities are allowed to utilize other operational or procedural control measures for protecting High and Medium impact ESPs. Even if a “nonprogrammable communication component” is defined as part of an ESP, it is possible that the “nonprogrammable communication component” will not reside within a defined PSP. It should also be noted that the addition of such language will result in increased burden for entities by nature of a backdoor requirement for documentation of all considered “nonprogrammable communication components” that are not NERC-defined “Cyber Assets.” The current proposed language applicable only to “nonprogrammable communication components located inside both a PSP and an ESP,” along with other PSP-specific requirements, may serve to discourage entities from creating defined PSPs around BES Cyber Systems.

No

The administrative burdens associated with this are not practical as a response and aligned with the risk introduced to the BES. KCP&L endorses those specific comments submitted by the Edison Electric Institute.

No

KCP&L believes that the definition of Transient Cyber Asset should be clear to ensure no unintended consequences from interpretations by stakeholders involved where direct connections of devices are anticipated. Physical and electronic access control to BES Cyber Systems is a critical component of securing the overall system, and such devices should be protected from inappropriate Transient Cyber Asset connections. But the definition of such lacks clarity and thus will lack consistency in application. The language around the Transient Cyber Asset and Removable media is silent and unclear where EACMS and PACS are concerned. The new definition could read as follows: Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Assets associated with an ESP. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Yes

While KCP&L supports alternative methods of assessing maturity and effectiveness in adherence to the NERC CIP requirements, the “Identify, Assess and Correct” language was an open-ended and unstructured framework that would cause confusion and lead to the expansion of the scope of NERC CIP based on auditor judgment. This concept would be addressed in tools and frameworks accomplished through the Reliability Assurance Initiative (RAI), however, consistency in auditor training and approach will be critical to the success of the RAI program.

Yes
No
We are not aware of additional jurisdictions that should be considered at this time.
Yes
KCP&L would like to endorse those comments made in this question by the Edison Electric Institute.
Individual
Scott Langston
City of Tallahassee
No
The City of Tallahassee (TAL) feels that Part 2.4 does not adequately illustrate the measures necessary to prove compliance to the part 2.4.2 requirement. The term 'representative sample' needs to be defined specifically. Does this imply a sample of rule sets from more than one access point? A sample of the rule set from a single access point? If more than one access point is identified, then would the entire rule set, or only a partial rule set from a single access point qualify as a representative sample? There can be no ambiguity when direct evidence is required as proof of compliance. Part 2.4.1 states that all external routable protocol paths, if any, must be through one or more identified access point(s). Evidence includes documentation of these paths through identified access points. If there is no requirement to discretely identify low impact BES Cyber Systems, then how can we be expected to provide evidence for this requirement when we are not required to identify the access point in the first place? External routable protocol paths imply the existence of an electronic security perimeter, a specific set of connected assets that form a basis for a defined network structure. There is no language in this requirement to identify an electronic perimeter, therefore no conceptual reason to identify an access point with routable protocol paths that may or may not be external to an undefined barrier. The language of this particular requirement and the measures required to prove compliance are extremely vague. Parts 2.1 – 2.3, and 2.5 are sufficient to address FERC Order No. 791 paragraphs 106-100, and clearly provide substantive objective criteria to sufficiently measure an entity's protection of low-to-no impact cyber assets. Requiring entities to identify assets (access points) where asset identification is clearly stated as unnecessary, and provide representative samples of configurations for these unidentified assets, assets that function as external access gateways to an undefined electronic security perimeter, could create an unnecessary quagmire of compliance effort. Under the section Guidelines and Technical Basis for part 2.4 it states that the Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. There is an assumption made here that at least one or more external routable protocol and/or Dialup connectivity paths exist and those access paths are being utilized to communicate directly with the asset from a remote location. This language should be rewritten to match the requirements in Part 2.4 – removing any unnecessary ambiguity with regard to direct communications pathways vs. other reasons for necessary connections via remote communications paths; e.g. "The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths, if any, to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected." Furthermore, the following sentence should be rewritten to state, "In cases where external connectivity is used to gain access to any low impact BES Cyber System at a remote site, electronic access controls should address the risk of using external connectivity." The final two sentences in this paragraph contain references to ambiguous concepts such as collection and aggregation, without stating specifically what kind of information might be collected and/or aggregated. TAL's contention is that these two sentences add nothing to the explanation and should be removed entirely. They state that these access controls are required to protect the collection and/or aggregation of low impact BES Cyber Systems, or the collection and/or aggregation of data pertaining to them, or what specifically?
Yes
No

Part 4.3 is identical to Part 4.2. I suggest collapsing 4.3 into 4.2 to include 'prior to use on applicable systems'. Both requirements are obviously meant to be done prior to use on applicable systems (intent of the standard in the first place), so there is no point in stating the same requirement twice. If the intent of this revision is meant to protect applicable systems, then the only requirement necessary is 4.3. If both requirements must stay, then remove the word 'detect' from 4.2 as detection is required prior to use as part of 4.3. It makes the most sense to collapse the two requirements into one and adjust the Measures language to include hardening policies and scanning techniques as part of the traditional antivirus … example.
Yes
No
I have no recommended alternative approach as I believe the original IAC language in the standard identified with a need to change industry perception of the spirit and intent of Critical Infrastructure Protection Reliability Standards to concentrate effective proactive compliance efforts towards identifying and correcting deficiencies rather than being focused on the fact that violations for those deficiencies may exist and subsequently turning the workplace into a reactive, audit documentation mill. The many changes in Violation Severity Levels in the revised standard will effectively result in potential violations regardless of any effort (or lack of effort) on the part of the entity to mitigate those violations. Now, with the IAC language removed, entities are no longer provided a much-needed greater degree of flexibility in detecting and remediating low-risk violations. All and any interpretation of the standards has been placed into the hands of auditors, which contributed to endless anxiety on the part of the entities with prior CIP versions. FERC stated concern over the broad and ambiguous nature of the IAC language as sufficient reason to force NERC to improve upon how the (IAC) language was written. As a result, NERC decided to assume that the enforcement process for low-risk violations would be unworkable, and remove the language altogether. This effectively disenfranchises the entity throughout the compliance auditing process.
No
Given the nature of the removal of the IAC language which results in a measurable change in how compliance programs would function under the new standard, FERC should issue an order to extend the effective date at least another full 6 months for each standard/requirement for which a modification to the language was made.
No
No
Group
Florida Power & Light
Mike O'Neil
Yes
Based on proposed revisions in the applicability section of the Generator Owner and Generator Operator Reliability Standards for PRC-005-2 (-3) and the approved CIP-002-5.1 Attachment 1 medium impact rating criteria 2.1, the following revisions to the applicability section of the CIP-003-6 Reliability Standard are recommended: Add a statement under 4.2.2 in the Facilities portion of the Applicability Section as follows: 4.2.2 Responsible Entities Listed in 4.1 other than Distribution Providers All BES Facilities. For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in

Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level. Proposed text for the guidelines and technical basis for this change parallels the text for similar changes to PRC-005-2 (-3): Applicability of the Requirements of CIP-003-6 to dispersed power producing resources is qualified in section 4.2.2. The intent is that for such resources, the Requirements would apply only to BES Cyber Systems used from the point where the BES dispersed power producing resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or higher and not at an individual turbine, inverter or unit level.
Group
Iberdrola USA Networks
John Allen
Group
Florida Municipal Power Agency
Carol Chinn
No
FMPA appreciates the SDT's efforts on this difficult task. We particularly appreciate all the outreach that the SDT has done with the stakeholders, beyond the normal development process outreach. Our comments and balloting positions are intended to be constructive and help improve the revised standards, so they will ultimately be approved. FMPA sees three issues with CIP-003-6. First, requirement R2 has been modified to remove the "IAC" language (as it has been removed from all other places in the CIP standards as well). This unfortunately has reintroduced a zero-defect tolerance due to the wording in R2. Second, while the standard states an inventory isn't required for low impact assets, use of the word "All" in part 2.4.1 implies that an inventory must be done in order to prove compliance. Third, while not a direct responsibility of the SDT, the RSAWs do not provide any level of clarity as to how the Entity can expect to be audited. FMPA suggests that R2 be reworded to address each of these three issues. FMPA proposes the following language (in a table format) to address the first two issues for R2: "Each Responsible Entity shall develop and institute Policies and Procedures designed to meet the following indicators of performance: • The Responsible Entity has an established, formal program for identifying Low Impact Assets. • The Responsible Entity has a process to evaluate the addition or removal of Low Impact Assets that can affect BES operations. • The Responsible Entity has a program to address the company's ability to detect and respond to compromise of the company's Low Impact Assets • The Responsible Entity has a program to provide training and awareness to all relevant employees. • The Responsible Entity institutes internal controls and procedures to prevent a recurrence of identified deficiencies This approach is based on the FERC "Policy Statement on Enforcement" Docket PL06-1-000. Specifically, it is taken from the Internal Compliance guidance that FERC has provided and has been instituted by the ERO in evaluating Internal Compliance programs through 13 standard questions. This approach would give entities a substitute for the IAC language promised in Version 5, plus give FERC the assurance that entities will have programs in place that can be audited. The Measures can be devised in a similar fashion to the grading system used by the regions to assess ICPs; and as such, the VSLs can be designed such that the requirement is measurable and "gradable". FMPA realizes that we are using the word "institute" in the above suggested language. We recognize that the SDT does not like to introduce new terms and/or language when possible, and FMPA supports that. The term "implement" was used in previous versions of the CIP standards. However "Implement" is not appropriate because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. By using the word "Institute", it would suggest that the policy is in force and able to be enforced by the Responsible Entity, but not requiring ERO enforcement of the policies in this requirement (implement includes enforcement), but rather ERO enforcement is contained in ensuing standards. Use of the word "implement" also introduces the zero defect problem because it can be argued that any defect is a violation of implementing a policy. Hence, a word that means that the entity has adopted and enforces adherence to policies is more appropriate, such as "institute" or "establish". FMPA suggests this approach for all requirements that formerly contained the "identify, assess and correct" language in Version 5. The removal of this IAC language introduces the zero defect issue. Yes, RAI is "promised"

as a solution to this problem; however, RAI is not “solid” enough for industry to depend on when supporting this standard and it is too important to depend on an unsubstantiated promise. In addition, FERC did not direct removal of the IAC language, but rather directed that the requirements be measurable and auditable. Our suggested alternative meets the FERC directive. If a complete re-write of R2 isn’t possible, FMPA has specific comments on some of the parts of R2. For part 2.4.1, using the word "All" in the requirement could be read to mean an entity has done a complete inventory of low impact assets in order to determine "all" of the communication paths suggested in part 2.4.1. FMPA suggests replacing the word “all” with “identified”, a la 2.4.2. Under part 2.5.1, FMPA does not agree with using the defined term "Cyber Security Incidents". We feel this could add to confusion, as the definition includes "Electronic Security Perimeter or Physical Security Perimeter". FMPA is aware there is an “or” qualifier on the definition that can be used to ignore the use of ESP/PSP terms that do not apply to Low Impact – perhaps having this information in the guidance part of the standard would clear up some confusion. FMPA also suggests limiting the scope of part 2.5 to Low Impact Control Centers and removing any reference that might include out-of-scope terms such as ESP's and PSP's. FMPA is also concerned at the lengthy wording of the VSL for CIP-003-6. With so many "or" statements, it may be difficult to follow. Since all the of the revisions for this balloting had the IAC language removed and there are limited RAI details available at this time, FMPA is voting negative on all of the CIP standards/VRF/VSLs posted for this balloting.
Yes
FMPA supports APPA’s comments on this question. APPA appreciates the SDT providing flexibility to entities in complying with R1 Part 1.10. Having multiple options for controls when physical access restrictions are not possible gives entities an opportunity to select the solution that works for their specific situation. Industry has commented that encryption of data as a sole solution may reduce reliability by adding complexity to the systems and latency to data flow that will not work in a relay control environment. If the SDT removes this flexibility or expands the applicability in future drafts APPA will need to reevaluate its support for the communications controls.
No
FMPA supports SMUD’s comments on this question. SMUD prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of “operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability)” as well as the corresponding Requirement Part 4.6 to “evaluate the Transient Cyber Asset.” SMUD believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a “defined acceptable use” for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. SMUD supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state “Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists.” As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source requirement part. SMUD is concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. SMUD does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. SMUD requests guidance be included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review.
Yes
No comments.
No
See comments under question 1 above.
Yes
No comments
No
No comments

No
In general the RSAWS need a significant amount of improvement. Given the removal of the IAC language in the standards, the RSAWS take on even more importance than before. The SDT could consider performing a non-binding ballot on the RSAWs as allowed for in the Rules of Procedure. At a minimum, the RSAW comments should be posted for transparency. A few specific comments on the RSAWs: • The RSAW for CIP-002 expands the standard greatly and we believe that an entity does have to list low impact assets in order to meet the RSAW requirements. • The RSAW for CIP-003 has a wrong number in 6a of R2.5 (bottom of page 19). It seems like the number 15 needs to be 36 calendar months in part “a” under the line item number 6 which has 36 in it. • We have some concerns with R2.5 items in the standard and at the bottom of page 19 of the RSAW. It adds in more criteria than what is written in the standard requirement (R2.5 and additional sub-requirements). We are unsure what R2.5.1 is asking for when it comes to “classification”. What if the auditor does not agree with our criteria for classification? What happens if we fail to identify a Cyber Security Incident (someone else identifies it)?
Individual
Nick Braden
Modesto Irrigation District
Individual
Chris Scanlon
Exelon Companies
No
In General: Exelon supports the SDT approach to add language to CIP-003, R2. Although we agree that the approach to add greater specificity to the required processes can fulfill the directive related to communication networks in Order 791, Exelon has concerns with the requirements as currently proposed. We are concerned that the revisions blur the distinction between low and medium impact and increase the burden for low impacts beyond the benefits to security and reliability. Exelon voted negative on CIP-003. Significant adjustments are needed for Exelon to support the revisions. Discussion of our concerns and some suggested revisions are offered below. Exelon notes that the low impact category is a comprehensive category bringing into scope all BES Assets that are not medium or high. This expansion of the CIP Standards is significant for the volume of newly covered assets brought into scope. Still, first and foremost, the emphasis, burden and investment of resources must focus on the assets most important to reliability and keep the burden of the requirements commensurate with the risk those assets pose to the Bulk Electric System. Exelon concurs with keeping all the requirements applicable to lows within one Standard (i.e. CIP-003). This Standard structure allows the requirements to include some unique features important to managing the low impact assets including: The specific language that no inventory is required The opportunity to set the compliance obligations at an appropriate level (i.e.; enterprise, site or program level instead of the device level) Exelon recognizes the value that one location for all low requirements may hold for entities with only low impact assets. As an entity with High, Medium and Low Impact assets, we would like the language to allow entities the option to fulfill certain requirements in CIP-003 R2 by incorporating Lows into their processes under associated standards applicable to Mediums. For instance, an entity should have the option to add Low Impact assets to their security awareness programs under CIP -004, R1.1 as a way to fulfill the CIP-003, R2.6 obligation. While not addressed in the proposed revisions, Exelon supports consideration of revision to the CIP-003 Applicability Section 4.2.2 to address dispersed power producing resources. It is important to clarify that security control requirements are set at the point of aggregation to 75 MVA and not at an individual turbine, generating unit or panel level for dispersed generation. The Project 2014-01 SDT is addressing similar concerns in other standards. Since the CIP V5 Revision SDT is currently revising CIP-003, it is a good opportunity to address this issue. Specific Concerns with proposed language: R2: While Exelon supports removal of the IAC language from CIP-003, R2 and the other requirements, our compliance concerns remain around the potential proliferation of compliance documentation, unreasonable compliance and enforcement burdens, and increased compliance risk. R2.1: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. R2.2: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”.

R2.3: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “Control Centers containing Low Impact BES Cyber Systems”. R2.3 Please offer more clarity on who is considered a “visitor” and the record keeping expectations/requirements for them. Discussion in the Guidelines will be helpful. R2.4: In general, R2.4 introduces significant complexity when applied to BES Assets with low impact BES Cyber Systems. This is concerning because even though FERC accepted in Order 791 (P.111) that creation and maintenance of an inventory of Low Impact assets for audit purposes would be unduly burdensome for Responsible Entities and could divert resources away from protection of High and Medium Impact assets, the currently proposed requirements make an inventory inevitable. We preferR2.4 to read similarly to R2.2 by stating: “Implement one or more documented processes that restrict logical access.” R2.4: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. R2.4.2: This subpart is problematic and an aspect that prevents Exelon from supporting the revisions. The administrative documentation burden associated with this subpart shifts the work of the control from protecting access points to documenting aspects of those access points. More problematic is the shift away from keeping the protections and compliance obligations commensurate with the risk posed by sites with low impact BES Cyber Systems. , These sites are low risk to the Bulk Electric System. The potential of the risk and the probability of the risk are low, and the protections in place at High and Medium Impact assets help diffuse the risks presented by the Low Impact assets on the system. The most valuable investment of time, resources, and personnel is in instituting protections at the High and Medium Impact assets and fulfilling the requirements associated with those BES Cyber Systems. R2.4.2 should be stricken. M2.4.2: Explain how the “representative sample” would be acceptable to demonstrate compliance. R2.5: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. Please also provide clear guidance stating that sites with low impact BES Cyber Systems may be covered by an enterprise-wide Cyber Security Incident response plan or other approach, and assurance that a Cyber Security Incident response plan is not required for each site. R2.6: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. R2.6: The proposed requirement language is confusing and seems more restrictive than its counterpart in CIP-004-5, R1.1. Naming the subparts as topic areas adds a compliance demonstration not present for Medium and High. The language should be clarified so entities understand the subpart topics are to be covered within the quarterly program so each of the subpart topics is covered at least once within 15 calendar months. In addition, R2.6 should allow entities with awareness programs under CIP-004, R1.1 to fulfill this CIP-003 R2 obligation through the CIP-004 program. Please consider adding to the Requirement: “If not already covered by fulfillment of CIP-004, R1.1, implement …” Compliance concerns: While Exelon supports removal of the IAC language from CIP-003, R2 and the other requirements, compliance concerns remain around the potential proliferation of compliance documentation, unreasonable compliance and enforcement burdens and increased compliance risk. Enforcing these requirements in a zero-defect approach could prove overwhelming for Responsible Entities and for NERC/Regional Enforcement. Reasonableness in the NERC compliance approach is essential. In some cases, the compliance expectations are influencing the applicability of the requirement language and contradicting language of FERC Order 791. For instance, Order 791 supported the importance of not requiring an inventory; however, the currently proposed language and under the current zero-defect compliance approach, there is not an obvious way to demonstrate compliance to the requirements without having an inventory. This makes the statement in the requirement ineffectual. The Order 791 directive concerning lows (P108) cites “an unacceptable level of ambiguity and potential inconsistency to the compliance process and an unnecessary gap in reliability.” While interrelated, addressing reliability and compliance are separate challenges. Order 791 did not object to the four issue areas as those relevant to apply to low impact assets for reliability. The SDT is challenged to refine the expectations around those control aspects. Concurrently, NERC is challenged to clarify the compliance process. While not the work of the SDT, the Reliability Assurance Initiative (RAI) and the RSAWs are companion pieces to the CIP standard revisions. Unfortunately, the initial draft RSAWs didn’t provide much clarity or relief from the zero defect compliance expectation; however, additional work on the RSAWs can help. Exelon encourages the RSAW development team to continue their work and post revised RSAWs with next iteration of CIP revisions. Concurrently, RAI could use the requirements applicable to Low Impact assets to demonstrate how RAI can alleviate the

compliance concerns and create a reasonable approach to compliance. This may be essential for the passage of revised requirements on Low Impact assets.

Yes

Exelon supports the SDT approach to add requirements to CIP-006 and CIP-007 to apply requirements to non-programmable communication equipment. We agree that this approach fulfills the directive related to communication networks in Order 791. Setting the protection requirements to within an ESP are appropriate and consistent with the components controlled by Responsible Entities. Exelon supports the decision not to define communication networks as a glossary term. The term itself is not used within the revised standards, but the revised requirements address protection of the nonprogrammable communications components identified in Order 791. Use of the terminology is understood within the context of the applicable standards (CIP-006 and CIP-007). Keeping the definition within the CIP context avoids implicating any additional Reliability Standards beyond the scope of the CIP revisions. By not creating a glossary term, the SDT avoids confusing broader discussions of communication networks that may be underway. While supporting the decision not to define communication networks, Exelon asks the SDT to consider whether it is valuable to define "non-programmable communication components." Exelon voted negative on CIP - 006 and CIP-007 to encourage the SDT to make additional refinements; however, Exelon generally supports the revisions. Some requested clarifications and suggested revisions are offered below. CIP-006, R1.10 should further clarify the scope to be only for ESPs with External Routable Connectivity. The relevant concern is with the external connectivity and in bridging PSPs. For settings that have an ESP without External Routable Connectivity, no PSP is required and therefore no bridging of PSPs can occur. The language should be revised to avoid creating an administrative burden that does not provide value. Consider adding to the CIP-006, R1.10 applicability "Medium Impact BES Cyber Systems with External Routable Connectivity at Control Centers and …" OR Revise CIP-006, R1.10 to read: "For ESP's with External Routable Connectivity, restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same ESP in those instances when …" Please confirm the understanding of the CIP-007, R1.2 applicability, "nonprogrammable communication components located inside both a PSP and an ESP" means the requirements apply to devices that reside within both and does not mean devices within a PSP and devices within an ESP. Discussion in the Guidelines could confirm if others seek confirmation of this intent.

No

Exelon supports the SDT approach to add requirements to CIP-010 and CIP-004 to apply requirements to transient devices and removable media. We agree that this approach fulfills the directive related to communication networks in Order 791; however, Exelon has concerns with the requirements as currently proposed. Exelon's concern is that, as currently proposed, there is additional administrative burden without sufficient benefit. The requirements should focus on addressing the relevant uses that present a potential to introduce malware, with emphasis on authorization/protections on the device at the time of connection rather than over various protection versions and use of the device rather than the people using it. We are very concerned that the requirements will obligate Exelon to track every use of a transient device regardless of whether contamination occurs or not. This concern is triggered primarily with the "prior to use" language (e.g., R4.6 "Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4") which indicates use here is every use, and thus must be tracked. The requirements on transient devices should not be more stringent than those on BES Cyber Assets. For example, R4.7 requires that TCAs be evaluated "within 35 days of use of the transient device to ensure patches are up to date" where the requirements for Medium and High BES Cyber Systems allow 35 days to evaluate and 35 days to patch. Exelon voted negative on CIP-010. Adjustments are needed for Exelon to support the revised CIP-010. Some requested clarifications and suggested revisions are offered below. CIP-010, R4.1-4.7: Applicability of the requirements should clearly apply to those Transient Cyber Assets and Removable Media (depending on sub-part) connecting to High and Medium BES Cyber Systems and their associated PCAs. Please consider revising the applicability column to read (depending on sub-part): Transient Cyber Assets/Removable Media connected to High and Medium BES Cyber Systems and their associated PCAs. CIP-010, R4.1 – Please clarify the expectations for authorization of users. Is this to be a list of individuals? If so, a list of names is an overly burdensome administrative task and a problematic compliance risk. The measures also do not seem consistent with the requirement language. The measure starts with the software or

configuration, while the requirement starts with users. The requirement logic should track with the measure by identifying the TCA first and then the authorization information. CIP-010, 4.1.4: Please clarify the expectations, if any, for tracking patch versions on a TCA and preapprovals required if 4.1.4 is updated per 4.6. “Defined acceptable use” in R4.1.3 is more relevant to security than the administrative nature of tracking patch versions. R4.1.4 should be stricken. CIP-010, R4.2 and R4.3 present a zero tolerance evidence challenge. Please discuss further the compliance evidence expectations. Exelon has no objection to being required to use methods to address malware on transient devices. Our concern comes in meeting the measures as written, which suggest evidence may be asked for each use of the process in each case. CIP-010, R4.4 – Clarification of the language is needed to distinguish between discovery of malicious code prior to connection and following connection of the device to a BES Cyber System. The relevant focus of the requirements should be on discovery of malicious code on connected devices and responsive mitigation. Consider revising R4.4: Mitigate the threat of malicious code detected during connection of Transient Cyber Assets and Removable Media. CIP-010, R4.5 is too rigid. Is the intent to require updating signatures prior to use? If so, consider modifying to read: Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns according to the Responsible Entity’s documented signature update process. CIP-010, R4.6 and R4.7 – While Exelon recognizes the added risk level associated with control centers, it’s not clear what circumstances these sub-parts seeks to capture in going beyond the intent of R4.1 and R4.2. Incorporating R4.6 into R4.1 and R4.7 into R4.2 may be warranted; however, this consideration should be given after thorough consideration of revisions to the proposed R4.1 and R4.2. Exelon understand that R4.6 seeks to apply an added authorization step for TCAs being connected to High Impact BES Cyber Systems and to Medium Impact BES Cyber Systems at Control Centers. Since this is associated with the authorization requirements in R4.1, it makes more logical sense to move this to R4.2. R4.7 seeks to allow latitude for Responsible Entities to make updates to TCAs according to a time schedule that may be dictated by other management practices other than a time just before use of the TCA. Exelon supports this flexibility. However, as currently written, the 35 days is more aggressive than for CIP-007, R2.2 and R2.3 that allow 35 days to evaluate and 35 days to install. Since both of these requirements apply to patching, the differences can limit the efficiency and effectiveness of an entity program that manages transient devices and BES Cyber Systems together. Please discuss the limitation of “per device capability” and any expectations for accommodating those without capability and/or any compliance expectations to demonstrate such capability. As presently proposed, Exelon finds the level of rigor placed on TCAs and RMs on par with that in CIP-007 applicable to permanent assets. The sentence in the rationale referencing the relative rigor should be removed.
Yes
No Commnet
Yes
Exelon supports removal of the IAC language from the 17 requirements and finds that this fulfills the Order 791 directive. Exelon continues to have questions regarding the RAI program and its fulfillment of the IAC intent.
No
The revisions to CIP-003, R2 are significant and as currently worded, represent a significant amount of work to implement the associated compliance program. The implementation plan should allow at least a year from the effective date of CIP-003-6. The Implementation Plan should make it clear that CIP-003-6, R2 will replace CIP-003-5 R2. The Implementation plan uses “months” and “calendar months”. Please clarify whether there is a difference between the two terms and, if no difference is intended, use one for consistency.
No Comment
Yes
Guidance: Exelon strongly encourages the SDT to write guidance to more fully explain the underlying intent of the requirement language. We recognize that guidance is not the same as the requirement language, but the information goes to the spirit of the requirement language and helps Responsible Entities establish their compliance programs to fulfill the requirements. Revision Development Timeframes: Exelon supports the SDT efforts to complete revisions in response to all four of the directive issue areas. In particular for the Low Impact asset requirements, completing the revisions will potentially enable Responsible Entities to implement the requirements with a clearer

understanding of the expectations and be able to do so once by skipping to implementation of V6. The Order 791-directed revisions are under development concurrent with industry work to implement the CIP Version 5 requirements, which is a daunting and resource intensive task. Iterative implementations are confusing and costly. RSAWs: (Restated from Q1) RSAWs are companion pieces to the CIP standard revisions. Unfortunately, the initial draft RSAWs didn't provide much clarity or relief from the zero defect compliance expectation; however, additional work on the RSAWs can help. Exelon strongly encourages the RSAW development team to continue their work and post revised RSAWs with next iteration of CIP revisions. RAI: Exelon supports the RAI concept and promise, but this is completely dependent on a greater understanding of and tangible experience with RAI. For Exelon and others, filling this gap may be essential for the passage of revised requirements, in particular for Low Impact assets. Regardless of the revisions, NERC has made commitments for RAI to be in effect in time for the CIP Version 5 implementation deadline. The revisions and RAI program components can work together. For instance, the IAC requirements may offer a useful vehicle to roll out to Responsible Entities the RAI aggregation concept to manage the requirements. As well, the Low Impact asset requirements are prime candidates to demonstrate how RAI can alleviate compliance concerns and create a reasonable approach to compliance for low risk requirement.
Individual
Rich Salgo
NV Energy
No
We generally agree with the approach that the SDT has taken, yet express the following concerns described below: Applicability The scope of dispersed generation in the applicability of this standard should be limited similar to that of PRC-005. We suggest the following be inserted within the section 4.2.2: "For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level." Requirement R2 The scope of R2 should be appropriately limited by restoring the reference to the assets identified in CIP-002-5.1 R1 Part 1.3. Suggest the following revision to R2: "Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required." Subpart 2.4.1 Clarification is needed that an external routable protocol past is "external" to the asset identified in CIP-002-5.1 R1, Part 1.3 containing low impact BES Cyber Systems. Suggest revising as follows: "All routable protocol paths to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems, if any, must be through one or more identified access point(s)." Subpart 2.4.2 As written, there is an implication that the use of a firewall is prescribed, as the term "by default" is used. Suggest revising Subpart 2.4.2 to read "For each identified access point, if any, require inbound and outbound access permissions, deny all other access, and document access permission reasons individually or by group." Part 2.6 As written in this draft, the specificity of what must be covered and the tracking of two time periods are more prescriptive than the requirements for Medium or High Impact BES Cyber Systems. Suggest the following language: "Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months."
No
General agreement; however, we request that clarification be added such that it is clear that entities are not expected to enforce CIP-006 requirements on third party non-programmable components that are not within the control of the entity.
No
We generally agree with the overall approach; however, we have specific concerns as described below. R4 part 4.1 We are concerned that Part 4.1 creates unnecessary administrative burden. For example, authorization generally applies to users. A user of a Transient Cyber Asset should be

authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also appears to overlap with CIP-004-6 R4 Part 4.1 which also addresses authorization.
No
The proposed definition for BES Cyber Asset, in conjunction with the Guidance of the Guidelines and Technical Basis create risk of misinterpretation. While a BES Cyber Asset is defined to “affect the reliable operation of the BES”, the Guidance dwells on the concept of BES Reliability Operating Services. If users interpret that to “affect” reliable operation is to be unable to perform a BES ROS, then certain devices whose loss could immediately preclude the BES ROS would have to be classified as BES Cyber Assets even though they likely do not affect the reliable operation of the BES. We suggest clarification in the Guidance that ensures perfect alignment with the definition. “Removable Media” definition lacks clarity that the portable media must be connected to “applicable systems”. Consider the proposed modification: “Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
No
While the SDT has removed the IAC language from these requirements in accordance with the directive, it nevertheless leaves the industry with an inevitable zero tolerance compliance enforcement paradigm, which is problematic, given that the new Reliability Assurance Initiative may not be in place. It is essential that compliance exception allowances be in place coincident with the removal of the IAC language from these 17 requirements.
Yes
There are references in the unmodified V5 Standards (CIP-002, 005, and 008) which continue to point to superseded versions of the modified Standards.
Group
Duke Energy
Michael Lowman
No
CIP-003: In Part 2.3 of the table, Duke Energy believes that it will be difficult for an entity to determine and monitor physical access points for Low impact BES Cyber assets. These access points may or may not exist for low impact BES Cyber Systems. We suggest the SDT consider requiring Low impact BES Cyber assets at Control Centers have a PSP in order to capture the intent of Part 2.3. In addition, we believe that requiring Low impact BES Cyber Assets to have the same control measures in place as Medium impact BES Cyber assets will become extremely burdensome for the industry and will provide little benefit to reliability. A distinction needs to be made between Medium and Low impact BES Cyber Assets. As an alternative, Duke proposes the following language for Part 2.4.2: "For each identified access point, if any, include the reason for granting access anywhere direct connectivity is allowed to or from the world-wide-web."
No
CIP-006: No comments CIP-007: We suggest the following revision to the Applicable Systems sections of Part 1.2 in Table R1-Ports and Systems: “High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components used for the connection between applicable Cyber Assets within the same ESP and within a PSP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components used for the connection between applicable Cyber Assets within the same ESP and within a PSP.” We believe this adds clarity on the expectations for nonprogrammable communication components.

No
CIP-010: (1)Duke energy suggests adding an additional bullet in the Applicable Systems section throughout CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection that states the following: • “A network within a PSP” We believe this is needed for consistency with the definition of Transient Cyber Asset. (2) We are unclear of the need to include 4.1.4 and 4.6 in Table R4. We fail to see the security and reliability benefit of this type of control method. As such, we suggest removing both 4.1.4 and 4.6 from the Requirements section of the CIP-010-2 R4 Table. CIP-004: No Comments
No
Duke Energy offers the following as an alternative suggestion for the definition of Removable Media: Removable Media: Portable media, directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact discs, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory. A Cyber Asset is not Removable Media. We believe the addition of “directly connected,” as well as items 1-3 provides more clarity and complements effectively the definition proposed for Transient Cyber Assets.
Yes
No
We suggest making the effective date of the Medium and High impact CIP standards enforceable on the same date(January 1, 2017). Also, we suggest that the Low impact CIP requirements should be enforceable one year later(January 1, 2018). The staggering of effective/enforceable dates as proposed, is confusing to industry stakeholders, and increases the likelihood of avoidable compliance violations. Whereas a consistent, across the board effective date, provides the clarity and consistency on the expectations for implementing the CIP Version 5 standards and revisions.
No
Yes
As stated above, we believe the CIP Version 5 standards and revisions should be effective on the same date for Medium and High impact requirements and a year later for low impact requirements. Again, we feel that having consistent effective dates may prevent compliance violations that can easily be avoidable.
Group
Peak Reliability
Jared Shakespeare
Yes
Yes
Yes
Yes
Peak supports the Standards as revised. However, Peak believes NERC/Regional Enforcement policies should be altered to allow entities to have low-risk, occasional non-compliance of certain NERC Standards without having to expend administration efforts on submitting Self Reports. Concrete threshold reporting criteria for certain Requirements should be set.
Yes
No

Individual
Heather Rosentrater
Avista
Yes
Avista supports the removal of the “identify, asses, and correct” language due to the expectation that NERC will refine its compliance and enforcement process under the Reliability Assurance Initiative (RAI) to move away from a zero tolerance approach to compliance. We expect the new RAI to be finalized prior to final ballot to address the zero tolerance concerns that the “identify, assess, and correct” language intended to address.
Individual
Don Schmit
Nebraska Public Power District
No
While we agree that protecting access to cyber assets is a valuable and a needed direction to move, we don’t believe that the additional level requirements for “Low” assets aligns with the associated risk to the BES. If assets are “Low”, then providing basic physical security and some fundamental access controls meets and is in line with the risk that classified them as “Low”. While the drafting team has tried to show in the guidance what would be acceptable and what would not, in essence they have determined the “how” the requirement will be audited by showing only a firewall solution. There are other methods to control access to facilities. The intent as we read it of the FERC comment was to have BES assets removed from direct internet access. Better language might be drafted that has utilities address that challenge, rather than force access control with firewalls for ALL low assets. This is an enormous burden increase for utilities as there are thousands upon thousands of devices to be covered as low impact, all with minimal risk to the BES. The burden on utilities will be immense as these devices are not static, and must be maintained, patched, and replaced every few years.
No
The FERC order did not require the removal of the IAC language; it does allow us to modify the language. We should either work through a solution together or remove the standard requirements entirely that contain the IAC language. As an industry, we need to find a better tool for reliability than to rely on zero tolerance in standards. We are spending too much of our time on very minor issues and it is diverting our attention away from focusing on the basics of reliability. The CIP standards quickly replaced all other standards as being the most violated due to the zero tolerance language in the standards. We would not have voted for version 5 without the IAC language. We are voting no on this version because the IAC language is being removed. To simply give up and remove it, because we can’t find a better compliance approach is disheartening. Reliability Assurance is a step in the right direction; however it is an enforcement action and not a compliance action. Simply removing the IAC language and saying Reliability Assurance will take care of the minor issues is avoiding the compliance solution. Even with Reliability Assurance, any issue is still a violation. The RSAWs for the proposed CIP Standards identify, at least 89 times for requirements and sub-requirements, where the auditor should find a violation. Reliability Assurance may help simplify the process with enforcement, but it is still a compliance violation. IT IS STILL A VIOLATION!!! The IAC language was attempting to take low risk issues and allow an entity to identify them and fix them

without any enforcement actions. Compliance, to the areas where IAC language was inserted, was tricky in version three; so we added IAC to provide a compliance solution to the requirements where we were constantly chasing violations with no value to reliability. As an analogy from our daily vehicle driving experiences, imagine driving in a vehicle where the speed limit is 45 mph. You approach a speed limit sign of 55 mph. A police officer is standing 10 feet in front of the 55 mph sign, clocks you at 46 mph and hands you a ticket for exceeding the speed limit. You're busted – you did exceed the speed limit in a posted 45 mph zone, but what is the value of the speeding ticket? Now, add NERC compliance to the speeding example and we are expected to self report each time we slightly exceed the speed limit in the above example. The value to public safety isn't controlling the speed of a vehicle that is going one mile per hour above the limit ten feet in front of a speed limit sign, but to prevent someone from excessive speeds that endanger others. Our court system and law enforcement officers have understood this for many years. Why can't we, as an industry, introduce some common sense into our reliability standards and remove zero tolerance? We remember implementing Urgent Action Standard 1200 for cyber security. We implemented the Urgent Action Standard to provide us some time to develop a sound program for cyber security. Many years ago, the need for action in developing cyber security standards was so great that we put the Urgent Action Standard in place to provide protection while we developed the NERC standards. We have deleted most of the Urgent Action Standard documents, but we did find one from February 2004 (over ten years ago). We implemented version one of the CIP standards years later. We have now approved version five and all the previous versions had similar pressures. Version 4 of the CIP standards was replaced before it was even effective. Now, we are working on version six of the CIP standards and want it effective before version five will be enforceable. What are we doing? As an industry, we are trying to implement version five, while maintaining zero tolerance to version three, but we don't know what version six will require us to do, but it will have the same effective date of version five. Does anyone wonder why so many companies are struggling with the CIP standards? We don't need to speed this version of the CIP standards through the system just to have to fix it later, like we have done with all the previous versions. We need to take our time, take a step back and try to get it right this time. We are sensing a lot of frustration in our industry over cyber security standards. The recent expedited development of CIP-014 diverted all of our attention and efforts this year, leaving little time to develop changes to the other CIP standards. We haven't implemented version five of the CIP standards, but we are already changing them before we have any experience with version five. Our recommendation is to slow down and get it right and not just try to get it done.
No
If the language as written for CIP-003-6 Requirement R2 is passed and remains unchanged, then keeping the implementation date of April 1, 2017 is not reasonable and will be difficult if not impossible for utilities to meet. Implementing access control at substations where there is none currently (or it is not as restrictive as the standards ask for) has the potential to cause failures or outages if not implemented carefully. There are numerous assets and logistical locations that would need to be addressed. Secondly, for some locations, implementing these measures may require facility outages that must be planned and coordinated months in advance, particularly in shared facilities. Larger entities will be working in 2015 to implement the High & Medium requirements, and will not turn their attention to "Low" requirements until that work is nearly complete. The resources implementing those requirements are in many cases the same ones that will perform the "Low" work, and their attention cannot be split without the potential for error. Additionally, since these changes will not be approved by FERC until late 2014 at best, we believe the effective dates should be extended using a simple calculation. From the time Version 5 was approved, to the time the changes are approved by FERC, that time should be added to the implementation date. For example, if the changes are approved in November 2014, then we add 1 year to the implementation dates. We would also suggest to make the implementation dates the same for all standards, and not have different implementation dates. It is additional administrative burden for both the entity and the auditor to have to keep a detailed tracking sheet of when each requirement is "effective". Make them consistent and the same to remove the potential error trap created with the multiple effective dates.
Individual

David Thorne
Pepco Holdings Inc.
It would be useful for users of the standards if the requirements for low impact assets outlined in the table for R2 were appended to the appropriate tables in the other CIP standards instead of CIP-003.
Yes
Pepco Holdings Inc. supports Edison Electric Institute's comments submitted for this project.
Individual
Bob Thomas
Illinois Municipal Electric Agency
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
ATC supports the current language, however, offers one suggestion for consideration. For consistency with the application of similar NERC Glossary terms used for higher applicable impact levels, ATC requests consideration of the addition of the word "interface" following the word "access point" where the term "access point" or "access point(s)" is used in Requirement R2 Part 2.4. in order to allow entities to identify with clarity where cyber ingress and egress controls are implemented for external routable protocol paths.
Yes
Yes
Yes
Yes
Yes
No
Group
PacifiCorp
Sandra Shaffer
No
Low Impact assets: PacifiCorp seeks to clarify that the external routable protocol path referenced in CIP-003-6 requirement R2.4.1 is 'external' "to the asset identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems" in the requirement. PacifiCorp also suggests that if the intent of requirement R2.4 is as suggested in the drawings provided in the Guidelines and Technical Basis, that additional language be placed in the requirement to align with the acceptable designs indicated in those drawings.
No

No
No
Transient Cyber Assets: PacifiCorp understands that the CIP-010-2 requirements are intended to apply to Transient Cyber Assets and Removable Media. Accordingly, to heighten clarity for the industry, PacifiCorp recommends that the Applicable Systems for CIP-010-2 requirements should be revised as follows: “Transient Cyber Assets directly connected (and/or as applicable by subpart) Removable Media connected to Medium (or High) Impact BES Cyber System…”, similar to the precedent for PACS in CIP-006-5 R1.1. PacifiCorp also recommends that the standards drafting team modify the requirement of “authorize” in CIP-010-2 requirement R4.1 to “document” as authorization implies additional administrative burden not even necessary for all of the applicable systems themselves.
No
Identify, assess, correct: It is PacifiCorp’s understanding that compliance exceptions and other Reliability Assurance Initiatives concurrently being developed by NERC are expected to adequately and appropriately address the industry’s zero defect concerns in place of the “identify, assess and correct” language that was removed by the 2014-02 standards drafting team. PacifiCorp believes that responsible entities deserve some certainty from NERC of the near-final or final form of these compliance exceptions and the mechanics to avail themselves of these exceptions, from a compliance and enforcement perspective, before they have to vote on these revised standards such that the industry can feel confident their concerns are being addressed.
No
No
Yes
Communication networks: PacifiCorp appreciates the standard drafting team’s revisions in relation to communication networks and does not have any suggestions for improvement of the draft language.
Individual
Karen Webb
City of Tallahassee
No
The City of Tallahassee (TAL) feels that Part 2.4 does not adequately illustrate the measures necessary to prove compliance to the part 2.4.2 requirement. The term ‘representative sample’ needs to be defined specifically. Does this imply a sample of rule sets from more than one access point? A sample of the rule set from a single access point? If more than one access point is identified, then would the entire rule set, or only a partial rule set from a single access point qualify as a representative sample? There can be no ambiguity when direct evidence is required as proof of compliance. Part 2.4.1 states that all external routable protocol paths, if any, must be through one or more identified access point(s). Evidence includes documentation of these paths through identified access points. If there is no requirement to discretely identify low impact BES Cyber Systems, then how can we be expected to provide evidence for this requirement when we are not required to identify the access point in the first place? External routable protocol paths imply the existence of an electronic security perimeter, a specific set of connected assets that form a basis for a defined network structure. There is no language in this requirement to identify an electronic perimeter, therefore no conceptual reason to identify an access point with routable protocol paths that may or may not be external to an undefined barrier. The language of this particular requirement and the measures required to prove compliance are extremely vague. Parts 2.1 – 2.3, and 2.5 are sufficient to address FERC Order No. 791 paragraphs 106-100, and clearly provide substantive objective criteria to sufficiently measure an entity’s protection of low-to-no impact cyber assets. Requiring entities to identify assets (access points) where asset identification is clearly stated as unnecessary, and provide representative samples of configurations for these unidentified assets, assets that function as external access gateways to an undefined electronic security perimeter, could create an unnecessary quagmire of compliance effort. Under the section Guidelines and Technical Basis for part 2.4 it states that the Responsible Entity must have implemented processes that

include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. There is an assumption made here that at least one or more external routable protocol and/or Dialup connectivity paths exist and those access paths are being utilized to communicate directly with the asset from a remote location. This language should be rewritten to match the requirements in Part 2.4 – removing any unnecessary ambiguity with regard to direct communications pathways vs. other reasons for necessary connections via remote communications paths; e.g. “The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths, if any, to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected.” Furthermore, the following sentence should be rewritten to state, “In cases where external connectivity is used to gain access to any low impact BES Cyber System at a remote site, electronic access controls should address the risk of using external connectivity.” The final two sentences in this paragraph contain references to ambiguous concepts such as collection and aggregation, without stating specifically what kind of information might be collected and/or aggregated. TAL’s contention is that these two sentences add nothing to the explanation and should be removed entirely. They state that these access controls are required to protect the collection and/or aggregation of low impact BES Cyber Systems, or the collection and/or aggregation of data pertaining to them, or what specifically?
Yes
No
Part 4.3 is identical to Part 4.2. TAL suggests collapsing 4.3 into 4.2 to include ‘prior to use on applicable systems’. Both requirements are obviously meant to be done prior to use on applicable systems (intent of the standard in the first place), so there is no point in stating the same requirement twice. If the intent of this revision is meant to protect applicable systems, then the only requirement necessary is 4.3. If both requirements must stay, then remove the word ‘detect’ from 4.2 as detection is required prior to use as part of 4.3. It makes the most sense to collapse the two requirements into one and adjust the Measures language to include hardening policies and scanning techniques as part of the traditional antivirus … example.
Yes
No
TAL has no recommended alternative approach as the original IAC language in the standard identified with a need to change industry perception of the spirit and intent of Critical Infrastructure Protection Reliability Standards to concentrate effective proactive compliance efforts towards identifying and correcting deficiencies rather than being focused on the fact that violations for those deficiencies may exist and subsequently turning the workplace into a reactive, audit documentation mill. The many changes in Violation Severity Levels in the revised standard will effectively result in potential violations regardless of any effort (or lack of effort) on the part of the entity to mitigate those violations. Now, with the IAC language removed, entities are no longer provided a much-needed greater degree of flexibility in detecting and remediating low-risk violations. All and any interpretation of the standards has been placed into the hands of auditors, which contributed to endless anxiety on the part of the entities with prior CIP versions. FERC stated concern over the broad and ambiguous nature of the IAC language as sufficient reason to force NERC to improve upon how the (IAC) language was written. As a result, NERC decided to assume that the enforcement process for low-risk violations would be unworkable, and remove the language altogether. This effectively disenfranchises the entity throughout the compliance auditing process.
No
Given the nature of the removal of the IAC language which results in a measurable change in how compliance programs would function under the new standard, FERC should issue an order to extend the effective date at least another full 6 months for each standard/requirement for which a modification to the language was made.
No
No

Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No
The proposed CIP-003-6 has language that is sometimes inconsistent with the larger framework of the CIP Standards. MMWEC suggests moving the requirements for security controls for BES Cyber Assets associated with Low Impact assets to the appropriate CIP Standards (CIP-004, CIP-005, CIP-006, CIP-008) and revising the language to more closely align with requirements for Medium and High Impact BES Cyber Systems. Additional table entries for applicability to groups of Low Impact BES Cyber Assets should be created as needed. To assist Responsible Entities that only own BES Cyber Systems associated with Low Impact assets, NERC should publish a guidance document that identifies Standards and Requirements that apply to Low Impact BES Cyber Systems. Comments specific to CIP-003-6 2.4 - By avoiding the concepts of Electronic Security Perimeters and Electronic Access Points, requirement 2.4 becomes difficult to interpret and less effective at protecting BES Cyber Systems from unauthorized access. We suggest more closely aligning the requirements for electronic access control with CIP-005-5 requirements for Medium and High Impact assets and moving the requirements to Standard CIP-005. This may require additional requirements, such as the identification of ESPs and EAPs. This may require Responsible Entities to expend more compliance effort than is currently proposed in CIP-003-6 R2.4. The Implementation Plan for these requirements should phase in enforcement over five years in order to address the challenges faced by Responsible Entities with large numbers of geographically dispersed Low Impact assets. This approach has been used in other NERC Standards that affect a large number of assets. (Examples include MOD-025-2, PRC-024-1, PRC-019-1 and others.) The Implementation Plan should require an increasing percentage of Low Impact assets to be compliant each year. Most Responsible Entities know the network architecture and communications capability of BES Cyber Systems associated with Low Impact assets. However, it will take time and resources to sufficiently document and, in some cases, implement additional cyber security controls on those BES Cyber Systems in order to be fully compliant with more stringent CIP Standards. A phased in approach to implementation plan will steadily increase the security of BES Cyber Systems over time.
Yes
MMWEC supports the changes to CIP-006 and CIP-007. However, CIP-006-6 should also include requirements for BES Cyber Systems associated with Low Impact assets.
No
MMWEC supports the comments submitted by SMUD regarding CIP-010 and Transient Assets. Also, CIP-004 should include training and awareness requirements applicable to BES Cyber Systems associated with Low Impact assets.
No
The definition for Removable Media should not be restricted to "portable." Also, the examples are unnecessary. Suggest the definition should be as follows - "Data storage media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data." The definition for Transient Cyber Asset should not include examples. Suggest the definition should be as follows - Transient Cyber Asset - A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset.
Yes
No
The Implementation Plan for requirements for BES Cyber Systems associated with Low Impact assets should phase in enforcement over five years in order to address the challenges faced by Responsible Entities with large numbers of geographically dispersed Low Impact assets. Entities with smaller numbers and Control Centers should be 100% compliant sooner than five years. This approach has been used in other NERC Standards that affect a large number of assets. . (Examples include MOD-025-2, PRC-024-1, PRC-019-1 and others.) The Implementation Plan should require an increasing percentage of Low Impact assets to be compliant each year. Most Responsible Entities know the network architecture and communications capability of BES Cyber Systems at Low Impact assets. However, it will take time and resources to sufficiently document and, in some cases,

implement additional cyber security controls on those BES Cyber Systems in order to be fully compliant with more stringent CIP Standards. A phased in approach to implementation plan will steadily increase the security of BES Cyber Systems over time.
Yes
Standards CIP-005 and CIP-008 should be revised to include requirements applicable to BES Cyber Systems associated with Low Impact assets.
Group
Tampa Electric Co.
Beth Young
No
Tampa Electric Company (TEC) participated in the development of Edison Electric Institute's (EEI's) comments on the Project 2014-02 CIP Version 5 Revisions and supports the comments as submitted by EEI for CIP-003 R2. TEC also supports the philosophy to provide objective criteria for CIP-003, Requirement R2 and recognizes the need to distinguish terminology in use for R2 from official NERC Glossary of Terms used in the other CIP Standards. For CIP-003, Requirement R2 Part 2.5, TEC recommends a rewrite; it is confusing to use the defined term Cyber Security Incident and Reportable Cyber Security Incident given that the definition only applies to one of the two scenarios that might identify an incident. Proposed alternative language: Utilize one or more programs to address the Registered Entity's ability to detect and respond to compromise of Low Impact BES Cyber Systems that may be discovered during the course of normal operations. If any deliberate or intentional disruption is discovered, the Entity should notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). At least once every 36 months, test the program used to detect and respond to compromises, conduct a lessons learned or after action discussion, and revise the program to address lessons learned or after action items. If CIP-003, Requirement R2 Part 2.5.6 remains as it stands, TEC recommends removal of the word paper to allow for other types of drills. For CIP-003, Requirement R2 Part 2.6, TEC recommends removing the language at least quarterly and changing the frequency to annual. We do not see that the risk related to the BES from personnel at locations with Low Impact BES Cyber Systems as deserving of the quarterly frequency.
No
For CIP-006, Requirement 1 Part 1.10, TEC considers that the second bullet monitoring the status of the communication link and issuing an alarm or alert is duplicative of the requirements that TEC follows in support of the reliable operation of the BES, specifically as required for COM-001-1.1 R1.1 (provide adequate and reliable telecommunications facilities including internally) and R2 (manage, alarm, test and/or actively monitor vital telecommunications facilities and equipment). TEC considers this requirement part of day to day operation of the Bulk Electric System and not prima facie evidence of a cyber security incident. Alternatively, TEC recommends changing the language of the bullet as follows: Where physical access restrictions to such cabling and components cannot be established, the Responsible Entity shall deploy and document alternative measures such as encrypting data that transits such cabling and components; or monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to appropriate personnel (such as those identified in the BES Cyber Security Incident response plan, Grid Operators within the Control Center, or other individuals charged with responding to the alarm or alert) within 15 minutes of detection.
No
Tampa Electric Company (TEC) participated in the development of Edison Electric Institute's (EEI's) comments on the Project 2014-02 CIP Version 5 Revisions and supports the comments as submitted by EEI related to CIP-010 R4 and CIP-004 R1, Part 2.1.9. In addition, TEC provides the following comments for consideration. TEC appreciates the efforts of the SDT to address the FERC Directives for transient devices drafted for CIP-010, Requirement R4. The language in Requirement 4.1 indicates that the authorization is taking place prior to the initial use which is a reasonable expectation. The Guidelines contain the following clarification : For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. This language in the Guidelines implies that R4 would need to be applied when a device moves between PSPs. This would have the potential to negatively impact the reliable

operation of the BES. Field technicians may be working on issues in one substation and get called to another location to address trouble tickets. Since these substations are not connected to the corporate network (and definitely not connected to the Internet), it would slow the process down if the technician needed to report back to a central location to validate the Transient Device between PSPs. TEC recommends clarification of the Standard and Guidelines to allow for a Transient Device to be validated on a periodic basis instead of on a per use basis between PSP or ESPs. For CIP-010 R4, Parts 4.3, 4.4 and 4.5, TEC is concerned that not all devices will be able to provide the documentation suggested in the RSAW related to the date Removable Media was used and provide adequate documentation related to the method used to detect malicious code. If there is no External Routable Connectivity, TEC is concerned that this requirement would necessitate the introduction of External Routable Connectivity to remote locations to support kiosks or other scanning devices along with expensive system upgrades in order to scan, update, log/track when the removable media was used, comply with this Requirement. The SDT should add the “per device capability” to CIP-010-2 R4 Part 4.3 to address device limitations. Similarly, TEC is also concerned there may be issues with the updates to the signatures under CIP-010 R4 Part 4.5. Since the Removable Media may be infrequently connected to either the corporate network or within a NERC ESP, we will have challenges in updating and tracking the date of A/V signatures on these devices. TEC is also concerned that not all types of Removable Media (Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.) can provide the ability to detect malicious code. TEC recommends that the subpart be updated to include the per device capability language used in other standards; this is implied in the Guidelines where the language includes the following: Part 4.5 requires a process to update signatures or patterns, where applicable. TEC recommends clarification of the Guidelines to allow for Removable Media to be validated on a periodic basis instead of on a per use basis. CIP-010-2 R4.7: For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use. TEC recommends the SDT include potential measures that would be appropriate to vendor Transient Cyber Assets and Removable Media.
Yes
Yes
While TEC is a strong supporter of the Identify, Assess, and Correct (IAC) deficiencies approach to NERC CIP compliance, we recognize the challenge of creating objective measures for the implementation of such a program. Therefore, we agree with the SDT direction to remove the IAC language as proposed. Our understanding is that the approach under consideration is the Reliability Assurance Initiative. There is a need for transparency and open dialog between NERC and Registered Entities related to implementation of the RAI. We expect the RAI to be finalized prior to final ballot to address the current zero tolerance compliance approach that the identify, assess, and correct language intended to address. TEC also recommends that the SDT consider a potential approach to address the removal of the IAC language via the Violation Severity Levels for a future revision, possibly adding thresholds to different levels.
Yes
Not applicable to TEC
Yes
TEC greatly appreciates the work of the Standards Drafting Team and the NERC staff. We support the efforts to have a consolidated revision to cover both the date sensitive and other FERC directives in a single filing. In addition, TEC respectfully requests the SDT consider the adoption of conforming changes in CIP-002, CIP-005, and CIP-008 to address the effective dates and version numbers in the background section to provide consistency.
Individual
Cheryl Moseley
Electric Reliability Council of Texas, Inc.
Yes
None.

Yes
Regarding CIP-006-6 requirement part 1.10, ERCOT requests a CIPC guideline on acceptable encryption protocols, methods, and key management. This could help auditors better understand acceptable practices and reduce the opportunity for individual interpretations by the CEAs. The language, “an equally effective logical protection” can be considered too vague and open to interpretation. Request that the language be modified as, “a compensating measure that provides an equally effective level of logical protection as the items listed above”.
Yes
None.
No
There appears to be a gap in the requirement language regarding media that is connected longer than 30 days (i.e.: permanent asset). Since it is not programmable, it would not qualify as a Cyber Asset and subsequently not become a BES Cyber Asset or BES Cyber System. There are situations where these types of devices are needed permanently, (e.g.: software licensing dongles, flash/USB drives storing bootable image files for appliances, etc.). Request that the 30 day duration be removed from the definition and require CIP-010-2 Parts 4.2 and 4.3 for all removable media. If the definition of Removable Media continues to be limited to 30 days, request a modification of the definition to address what the media is plugged into, similar to Transient Cyber Asset. Recommended definition: “Portable media, connected for 30 consecutive calendar days or less to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset, in order to copy, move and/or access data.” Also, recommend the definition be modified to as: “Removable Media is not a Cyber Asset.”
Yes
None.
Yes
None.
None.
None.
Group
Western Area Power Administration
Lloyd A. Linke
No
The “external routable protocol paths” language in Requirement 2.4 requires entities Low Impact Cyber Systems to provide and comply with “some form of electronic security perimeter,” regardless of risk to the Bulk Power System/Bulk Electric System. Compliance to this requirement would be excessive given the risk associated with Low Impact rated BES Cyber Systems. The language in the CIP Requirements is confusing. On one hand, entities would be required to identify, maintain and comply with “some form of electronic security perimeter” (ESP) for Low Impact rated BES Cyber Systems, on the other, CIP Version 5 (or the proposed Revisions) states that “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” This is contradictive at best and should be clarified. Recommend language changes to address only Low Impact Systems which have direct internet access. Recommend adding language which assesses risk to Low Impact BES Cyber Systems with “external routable protocol paths.”
Yes
No
No
It would make more sense if the implementation were after the CIP Version 5 Standard implementation dates.
Yes

Yes
Recommend that the CIP Standards be aligned with Risk to the BES and that the object of the Standards be clarified. In many cases the SDT refrains from clear language so as not to dictate a particular approach. This leaves the interpretation up to Entities and Auditors who don't share the same perspective. We recognize and appreciate that SDT doesn't want to dictate activities. If the risks being mitigated are clearly understood that could provide the necessary clarity without eliminating varied approaches including technological advances.
Individual
Thomas Foltz
American Electric Power
No
The current wording of CIP-003-6 R2 Part 2.4 should be revised to align more closely with the definition of External Routable Connectivity. Suggested wording: “2.4.1 All bi-directional external routable protocol paths must be through one or more identified access point(s).” If the suggested wording is accepted by the drafting team then the Guidelines and Technical Basis should be revised as well to include the bi-directional clarification. The measure for item 2.4.2 should be revised to remove data diodes. A data diode is not an access point to a low impact BES Cyber System if it is configured in a manner that only transmits information outside the BES Cyber System. There are no inbound access permissions that can be applied since the device is hardware limited. Documenting how outbound traffic is sent provides no security benefit to the BES and would be an unnecessary administrative burden. The current wording of Part 2.6 could be read as a quarterly requirement for the reinforcement of cyber security practices and the 15 calendar month enforcement of Parts 2.2, 2.3, 2.4, and 2.5 above. This wording is more prescriptive than the wording for high and medium impact BES Cyber Systems. The wording should be revised to better align with the CIP-004-5 R1 Part 1.1 wording. This would give the entity the flexibility to determine what items need to be included in its security awareness program based on the current threat environment or detected lapses in cyber security practices. Suggested wording for the 2.6 Requirement – “Implement a security awareness program(s) that reinforces cyber security practices at least once each calendar quarter.” In addition, the wording is confusing in 2.3 – 2.4. If the site has a defined physical boundary (DPB) are the devices outside of the DPB in scope if they are low? Is it possible to define a DPB inside of a building as a site versus the whole site?
No
CIP-007 R1 overlaps with CIP-010 R4. We suggest removing the language from CIP-007 R1.
No
Requirement R4 represents a significant administrative burden. The fact that Transient Cyber Assets and Removable Media are not connected for extended periods of time to a BES Cyber System makes the automated logging and tracking of these devices impractical. To make this a more manageable requirement with less administrative burden Requirement Part 4.1 should be removed or modified to apply to medium impact BES Cyber Systems with External Routable Connectivity. This would align the requirement part with CIP-004-5 regarding the authorization of user access. User authorization is only required for high impact and medium impact with External Routable Connectivity BES Cyber Systems. The authorizing and tracking of Transient Cyber Assets will add a significant documentation burden with minimal increase to cyber security. The most significant threat Transient Cyber Assets pose to BES Cyber Systems is the potential to be a gateway to introduce malicious code. Requirements Parts 4.2, 4.3, and 4.4 should be sufficient to address these concerns on high and medium impact BES Cyber Systems without adding a significant administrative burden. Requirement Part 4.4 appears redundant to CIP-007-5 Requirement 3 Part 3.2. The current wording reads as if the threat of detected malicious code on high or medium impact BES Cyber Systems be mitigated. Suggested wording: “Mitigate the threat of detected malicious code on Transient Cyber Assets and Removable Media associated with or that could be connected to applicable systems.” This will make it clear that the mitigation actions in regards to Part 4.4 need to be conducted on the Transient Cyber Asset and Removable Media. Requirement Part 4.7 suggested wording: “Evaluate Transient Cyber Assets prior to use for security patches related to Part 4.1.4. For security patches that are not up to date take one of the following actions:…..” In addition, AEP would recommend highlighting or separating out the unique differences between these requirements and the ones

earlier in the CIP-010 standard. Also, do the devices have to be dedicated to the ESP and not used on other networks?
Yes
It is unclear why TCAs are being associated with Removable Media in the standard.
Yes
Yes
As long as the timeframe for implementing Low impact systems is not shortened, and the guidance is released with significant time to bring the Low impact systems into compliance.
No
No
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Group
Large Public Power Council (LPPC)
Joe Tarantino
No
The addition of more objective criteria for Low impact BES Cyber System Requirements within CIP-003-6, R2, breaks one of the prime objectives defined when CIP version 5 was being developed that each of the Standards could stand on its own. For entities with Low “and” either Medium or High Cyber BES Cyber Systems, it would be necessary that CIP-003 “always” be referenced when any of the requirements in CIP-004-6 through CIP-011-2 when the Medium and High impact BES Cyber Systems are being designed and implemented, since dependencies are always possible between BES Cyber Systems and the parts of any impact category. It is customary in other control objective families to present controls together, but identify whether there are different impact levels. The CIP standards have implemented this approach using the Applicable Systems table. SMUD appreciates the concerns from smaller Low impact only asset owners that there is far more requirements for Medium and High impact assets than there is for Low impact. Without sacrificing the integrity of maintaining the control objectives together and facilitating a directed set of controls to the Low impact owners, SMUD would recommend to NERC to develop specific targeted outreach documents for these entities that present just the Low impact asset control objectives in a more simplified manner. For example, at SMUD we have different groups that manage certain types of devices such as Electronic Access Control and Monitoring Systems (EACMS). We have created a presentation of a subset of Requirements and Requirement parts that just cover the EACMS so that those subject matter experts have a document for just those items that affect the applicable systems they manage. Additionally, to support this approach from an audit perspective, specific RSAWs could be created for the Low impact requirements that reduce the number of RSAWs that need to be completed by the entities. The inclusion of these objective requirements with a unique table in CIP-003-6 result in Standards language inconsistencies that creates confusion and additional compliance risks. A new definition is now needed for CIP-003-6, R2, Requirement Part 2.4 for the phrase “external routable protocol paths” to ensure that entities and auditors clearly understand the differences between that phrase and the defined term External Routable Connectivity. This would avoid duplicating the confusion seen in earlier versions of the CIP Standards, such as the CIP-002 confusion between Facilities and facilities. The phrase “external routable protocol paths” may create a similar interpretation risk. SMUD recommends that the language added to CIP-003-6, table R2 for Low impact assets be moved to the specific tables in each of the Standards CIP-004-6 through CIP-011-2 where applicable. Specifically, SMUD recommends the following: 1. CIP-003, R2, be modified to return the policy language to: “Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part 1.3, shall implement one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months. 2.1 Cyber Security Awareness; 2.2 Physical

Security Controls; 2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and 2.4 Incident Response to a Cyber Security Incident." This allows the entity to develop specific policies that are relevant to these areas; which is consistent with the intent of the CIP-003 standard. The objective criteria is then moved into the relevant CIP standards. SMUD believes that there needs to be guidance included for entities that also have Medium and/or High impact facilities that acknowledges a separate set of specific policies just for Low Impact is not necessary. Entities are permitted to leverage the policies for Medium Impact and/or High Impact and add the Low Impact applicable requirements. 2. CIP-003, R2, Part 2.1 would be removed and rolled into the Requirement 2 language. 3. CIP-003, R2, Part 2.2 would have Low Impact BES Cyber Systems added to CIP-006, R1, Part 1.1 Applicable Systems table. 4. CIP-003, R2, Part 2.3 would be added to the CIP-006, R2 Visitor Control Program table with a new Part applicable to Low Impact BES Cyber Systems. 5. CIP-003, R2, Part 2.4 would be added to CIP-005 as a new Requirement 3 with each of the current 2.4.1 – 2.4.3 as new Requirement Parts. 6. CIP-003, R2, Part 2.5 would have Low Impact BES Cyber Systems added to the CIP-008 standard maintaining the 2.5.6, 36 calendar month timeframe specific to Low Impact BES Cyber Systems. Additionally, for the existing CIP-008, R3, Requirement Part 3.1 extending the 90 date update cycle for Medium and High Impact BES Cyber Systems to 180 days for Low Impact BES Cyber Systems. For incident response, the SDT presented all but three of the CIP-008 Requirement Parts: 2.2 – Use the Cyber Security Incident response plans(s); 2.3 – Retain records related to Reportable Cyber Security Incidents; 3.1 – set an update frequency to the Plan. SMUD believes that requiring these three other Parts do not impose a significant burden for entities with Low Impact BES Cyber Systems. SMUD believes extending the update cycle for Part 3.1 to 180 days for Low Impact BES Cyber Systems is an appropriate timeframe based on the risk to the BES. 7. CIP-003, R2, Part 2.6 would be added the CIP-004, R1 Security Awareness Program table with a new Requirement Part 1.2 applicable to Low Impact BES Cyber Systems. The language would be updated to read: "Security awareness that, at least once each quarter, reinforces cyber security practices (which may include associated physical security practices)." The proposed language from CIP-003, R2, Part 2.6 created a higher performance requirement than for Medium and High Impact BES Cyber Systems by requiring the specific Low Impact BES Cyber Systems items to be specifically covered each year. 8. With the addition of the CIP-003, R2, Part 2.4 requiring an "access point" for Low Impact BES Cyber System, the exemption for Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters" in the Introduction section, number 4.2.3, Exemptions needs to be updated to include Low Impact BES Cyber Systems since Low Impact BES Cyber Systems do not require an Electronic Security Perimeter, but it still needs to be clear that the stated exemption is still in place for the Low Impact BES Cyber Systems.

Yes

No

SMUD prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of "operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability) as well as the corresponding Requirement Part 4.6 to "evaluate the Transient Cyber Asset." SMUD believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a "defined acceptable use" for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. SMUD supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state "Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists." As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source Requirement Part. SMUD is concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. SMUD does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. SMUD requests guidance be

included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review. One approach to removing use is that for those entities that only use their transient devices a few times a year, they can assess for patches “once every 35 days,” but prepare a mitigation plan that they will install the patch at the next use and assign a date for the mitigation plan. This does not impose the tracking of use related to transient devices and accommodates both approaches for those entities that have included their transient devices within their normal security patch processes and those entities that only use their transient devices on an irregular schedule.
No
SMUD supports the need for definitions associated with Removable Media and Transient Cyber Assets. In reviewing the proposed definition for Removable Media, SMUD believes additional clarity is needed to ensure the definition encompasses the appropriate components. SMUD requests removing the word “portable” from the beginning of the definition and adding “capable of removal without powering down the system” to the beginning of the definition. This removes a need to create a further definition of “portable” and ensures the equipment such as hot-swappable hard-drives are also included. The full requested text of the definition is below. “Removable Media: [delete:"Portable"] Media [add:"capable of removal without powering down the system,"] connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.”
Yes
SMUD supports the SDT removal of the IAC and fully supports the efforts of NERC to develop the Reliability Assurance Initiative (RAI) program. SMUD supports the shift from a zero-defect enforcement approach to a risk based method and providing alternative paths of enforcement.
Yes
No
No
Group
DTE Electric
Kathleen Black
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
There is concern regarding the faxct that the physical security requ9rements for lown mpace cyber sysrtems were put into CIP003 rather than CIP006. As we have seen repeatedly in the past, breaking up similarlysituated provisions into different CIP standards creates an interpretative and

administrative burden. It would be recommended that all physical security requirements should be in CIP006 to eliminate any confusion.
Individual
Karin Schweitzer
Texas Reliability Entity
No
All of the criteria in Table R2 are procedural with no performance requirement regarding the inventory of low-impact BES cyber systems. Texas RE recommends that specific performance requirements be added.
No
CIP-006, Requirement R1 Part 1.10--the requirement contains language that is not clear and therefore does not pass the test for NERC's "Acceptance Criteria of a Reliability Standard," item 8. The requirement of "an equally effective logical protection" is ambiguous and does not lend itself to a consistent interpretation of the required performance. If a responsible entity chooses to implement what it considers to be "an equally effective logical protection" (since it is only required to implement one item listed in Part 1.10), it is possible that a reliability benefit will not be achieved.
No
CIP-010, Requirement R4--it is unclear if the word "policies" in the Measures section of Requirement 4.2 is intended to mean application policies or a written policy that requires someone to take a certain action. Texas RE recommends that the SDT clarify the use and intent of this term.
Yes
Yes
Yes
Yes
Entities should be required to demonstrate evidence of the effective execution of controls and not just that they have a policy or procedure.
Individual
Heather Bowden
EDP Renewables North America LLC
Yes
Yes
Yes
Yes
Yes
Yes
No
Group
SRC

Greg Campoli
Yes
The SRC & SWG agrees in general with the requirement approach. Additional considerations below: CIP-003 R2 • p. 8, Since the phrase “external routable protocol path” has significance in the applicability of this standard and has a peculiar meaning, it should be added to the NERC glossary. • p. 8, “The Standard Drafting Team (SDT) intent in using the phrase ‘external routable protocol paths’ is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).” Does this imply that the phrase does not account for paths from the low impact BES Cyber Systems? • p. 8, “for its assets containing low impact BES Cyber Systems”. What does “containing” mean in this context? The asset is a BES Cyber System or is not. It does not “contain” a BES Cyber System. Suggest changing it to “for its assets that constitute BES Cyber Systems.” There should also be a comma following “[e]ach Responsible Entity” and “BES Cyber Systems” in the first sentence. • R2 Note on page 9 – If a list of low impact BES Cyber Systems is not required, how can this requirement be audited? This statement worked for a policy, but not for the new sub requirements, which must be “performed.” • Table R2 contains a scaled-down cross-reference to other requirements. This should be accomplished by adding “Low Impact BES Cyber Systems” in the Applicable Systems column of applicable requirements rather than setting apart a separate set of requirements for low impact BES Cyber Systems. • R2.5 – Will this require a separate plan or can it be addressed in the CIP-008 plan? Please explain in rationale or guidance.
Yes
The SRC & SWG agrees with the requirement approach. Additional considerations below: CIP-006 R1.10 • Use of encryption should be restricted to approved protocols and methods. Should there be requirements around key management? How will this be audited? • It is not clear in the Requirement text whether an entity can simply choose not to implement physical access restrictions or if it must demonstrate that it cannot for some reason. Although the text leaves open the possibility that physical, as opposed to logical, protections are optional, the phrasing can also be read to imply that restricting physical access is a preferred or default measure. Although the accompanying guidelines state explicitly that entities may implement physical or logical measures, the requirement itself is not as explicit • It is not clear how Regional Entities will assess whether a logical protection is “equally effective.” Will the REs defer to an entity’s judgment, or will there be a process by which entities can receive assurance that a logical protection is sufficiently robust to be “equally effective”? If entities must wait until their next audit to find out whether a measure is equally effective, they may simply ignore this option despite being permitted to develop such measures. More guidance should be provided on what is acceptable (pp. 36-37)
Yes
The SRC & SWG generally agrees with the requirement approach. Additional considerations below: CIP-010 • R4.1 Authorization should include purpose for connecting the TCA, start date/time, duration, and which ESPs the TCA is authorized to connect to. Also, the “caution” on p. 42 should be woven into the requirements that TCAs must be configured not to allow network bridging via wireless or blue tooth. It should be a required configuration check prior to connection. • In Requirement 4, Part 4.1.4, the term “intentionally installed software” is vague. For instance, the accompanying guidance suggests that “notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software” are not intended to be listed in the authorization of a Transient Cyber Asset. However, such an exception is not evident from the requirement language itself. Instead, the term “intentionally installed software” could be reasonably interpreted as covering all software on a Cyber Asset other than malware or other malicious programs. We recommend that the phrase be revised to provide greater specificity with regard to the types of software that should be included in the authorization. • R4.3 Why is there no “deter” or “prevent” for Removable Media? These are required for TCAs. • Malware should be grouped together in CIP-007, not split up in different standards. • In Requirement R4.4, the phrase “mitigate the threat” is ambiguous. For instance, it is unclear what constitutes mitigation after malicious code is detected or what the timeline for such mitigation is. (On the latter point, the current language does not even require that such mitigation be completed prior to use.) We recommend that a specific outcome for such mitigation be clearly expressed as well as language indicating the required timing of such mitigation. • R4.6 – This remediation or updating should be done prior to use as well. Should be more explicit. Could be a loophole. • In

Requirement R4.7, it is unclear whether a single evaluation within 35 days prior to use would be sufficient to comply with the requirement or if the requirement's emphasis is on "ensur[ing] security patches are up-to-date." In addition, it is not clear if a monthly evaluation would be sufficient regardless of how often the Transient Cyber Asset is used, e.g. if an evaluation must be performed prior to each use or if a single evaluation covers all use occurring within 35 days afterward. The accompanying guidance suggests that "rolling" evaluations are acceptable, but the requirement language itself is vague on this point. It may be advisable for the SDT to delete Requirement 4.7 and instead add Transient Cyber Assets to the Applicable Systems for the existing patch management requirement.
Yes
The SRC & SWG agrees in general with the revised definitions. Additional considerations below: • May want to include tape as an example of Removable Media. • Removable Media: need to clarify with respect to what it's connected to, as seen in the definition for Transient Cyber Asset. • BES Cyber Asset and Protected Cyber Asset include clarification on definition of Transient Cyber Asset. These statements should be moved to the definition of Transient Cyber Asset and not woven into other definitions. • Removable Media: Given that Removable Media are not Cyber Assets, if one is connected for more than 31 consecutive days, what happens? Is it somehow subject to certain requirements? • Removable Media: "A Cyber Asset is not Removable Media" – Is this trying to say that Removable Media is not a cyber asset? Need more clarity on this. • What happens if a TCA is connected for more than 30 consecutive days? Is it still a TCA, a BES Cyber Systems, or an undefined asset that is not subject to requirements? • The definition of Removable Media should at least be revised to state that "Removable Media are not Cyber Assets."
Yes
Comments: SRC & SWG agrees with the requirement The approach. Additional considerations below: • When will we see a specific description of the RAI program as applied to CIPv5 standard compliance enforcement and expectations of RE's for collecting evidence to support the RAI process?
Yes
The SRC & SWG agrees with the requirement approach. No additional comments.
Yes
The Canadian SRC & SWG members are not aware of any other provincial or regulatory requirements that need to be considered at this time.
Yes
• The present redline changes to standards look fine as far as addressing FERC's directives for changes to the CIPv5 standards. The SDT is to be commended for bringing these changes to a reasonable state for review and ballot in such a short period given the subjects involved. • There is concern that that the different versioning of the standards may cause confusion. It would be clearer for all to be promoted to the same base version 6.
Individual
Dale Dunckel
Public Utility District No. 1 of Okanogan County
Group
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Pamela Hunter
No
Southern Company agrees, in part, with the approach for meeting the FERC directive addressing more objective criteria around protections for low impact BES Cyber Systems. Southern fully supports the continued use of the language eliminating the overwhelming burden of creating and maintaining lists of low impact BES Cyber Systems or Assets and lists of authorized users with access to low impact BES Cyber Systems. In addition, Southern fully supports the revisions under CIP-003-6 R2.3 being specifically applicable to Control Centers containing low impact BES Cyber Systems, and the incident response plan testing timeframes (once each 36 calendar months) under CIP-003-6 R2.5. However, Southern will be submitting a "No" vote on the revisions to CIP-003-6 R2 for the following reasons: 1) In the change to the tabular format, the requirements now imply that

they are at the individual low impact BES Cyber System level, rather than at the “Assets containing Low Impact BES Cyber Systems” level. The Applicable Systems column should be amended to state “Assets containing Low Impact BES Cyber Systems.” 2) Under CIP-003-6 R2.1, consider allowing approval of the cyber security policy or policies addressing CIP-003-6 R2 by the CIP Senior Manager “or delegate.” 3) Consider limiting the scope of CIP-003-6 R2.5 to “Control Centers containing Low Impact BES Cyber Systems.” 4) CIP-003-6 R2.5.6 – consider removing the word “paper” in front of “paper drill” to allow for various types of drills to be performed for incident response exercises. 5) Consider the following revisions to CIP-003-6 R2.6: “Implement a security awareness program that reinforces cyber security practices at least once each 15 calendar months” and remove the requirement to reinforce the previous requirement Parts. 6) Consider providing additional clarity in the Guidelines and Technical Basis section on what constitutes “external” in the context of the term “external routable protocol paths.” Is this strictly external to each asset containing low impact BES Cyber Systems (i.e., is every Cyber Asset at the asset considered “internal”)? 7) Consider providing additional information in the Guidelines and Technical Basis section on the use of the term “Cyber Security Incident” as it applies to low impact BES Cyber Systems. Although the defined term uses an “or” statement that would keep the scope of the definition applicable to low impact BES Cyber System, this should be explicitly noted. Southern Company also supports the following GTC comments to this question: GTC is concerned that by borrowing language from Medium Impact requirements, the SDT has introduced a substantial increase in administrative overhead to comply with the standard without an equivalent increase in security. Specifically, maintaining the documentation overhead of justifications for every firewall rule results in a significant amount of man-hours devoted to compliance and not to improving the security of the low impact BES Cyber Assets.
Yes
Southern Company agrees with the approach with meeting the directive in FERC Order No. 791 addressing protections for non-programmable components of communications networks.
No
Southern Company does not agree with the approach taken to address transient devices (Transient Cyber Assets and Removable Media). The new CIP-010-2 R4 requirements place an unachievable amount of responsibility and overwhelming administrative burden on Responsible Entities, specifically with regard to the handling and measures required for cyber assets that are not owned or maintained by the Responsible Entity, but for which there is significant dependence in order to ensure reliable operation of the Bulk Electric System. These new Standards, as well as the Guidelines and Technical Basis addressing these new Standards, strive more towards the prohibition of the use of TCAs and Removable Media, rather than providing achievable security Standards that a Responsible Entity could successfully implement. Southern Company provides the following comments to the SDT for consideration: 1) The Measures of CIP-010-2 R4.1 only address requirement R4.1.4 applicable to authorized baselines of TCAs and do not address examples of evidence for authorization of Users, Locations, or acceptable use, nor examples of how a Responsible Entity can demonstrate “prior to initial use.” 2) CIP-010-2 R4.1.2 – Southern recommends that acceptable use should not be required to be “authorized” for each initial use of a TCA, but should be separated to allow for addressing acceptable use at the policy/procedure level. See the below comments for additional recommendation/revision. 3) Under CIP-010-2 R4.6, where the requirement calls CIP-010-2 R4.1.4, the Applicable Systems are different between the two requirements. The Applicable Systems under CIP-010-2 R4.1 should either be changed from Mediums to Medium Impact BES Cyber Systems at Control Centers and their associated PCAs to match R4.6, or CIP-010-2 R4.6 should be re-written to include moving R4.1.4 into R4.6. Consider the following: CIP-010-2 R4.1: Define acceptable use of Transient Cyber Assets, and the process to authorize usage of Transient Cyber Assets, except for CIP Exceptional Circumstances. Authorization shall include: R4.1.1 - Users, individually or by group/role; R4.1.2 – Locations, individually or by group/role. CIP-010-2 R4.6: Evaluate TCAs, prior to use, and document the authorized baseline configuration of the TCA. Evaluation shall include authorization of: R4.6.1 – OS, Firmware, and intentionally installed software on TCAs (per Cyber Asset capability); R4.6.2 - For a modification that deviates from the state in Part 4.6.1, either: Remediate by returning the TCA to the state in Part 4.6.1; or Update Part 4.6.1. If the above suggested language is considered and/or included, the comments on changing the Applicable Systems under R4.1 may be ignored – no change to the Applicable Systems in R4.1 or R4.6 would be necessary given these revisions to R4.6. 4) Requirement R4.1 places a lot of

overhead on the Responsible Entity to simply maintain lists, rather than contribute significantly to security or reliability. Southern Company requests consideration that requirement R4.1 and R4.6 be applicable to just High Impact BES Cyber Systems and their associated PCAs. 5) The requirement to authorize and inventory all software on a TCA places an undue burden on those instances where a vendor needs to use their devices with their proprietary or licensed software in order to maintain or upgrade a BES Cyber System to maintain reliability. We suggest the SDT give thought to how a Responsible Entity can "authorize" proprietary hardware/software on a vendor TCA when the RE has very limited control over that device and limited or no understanding of the proprietary software contained therein. How can a Responsible Entity reasonably be expected to prove "initial use?" Does it serve a greater reliability purpose to tell vendors they cannot use their proprietary hardware or software to maintain BES assets? Or that they must buy another license of any licensed software so it can be installed on the Responsible Entity's TCA device? While we understand this is an area of increased risk, we suggest that checking patch levels and updated anti-malware use on the TCA (per Cyber Asset capability) is sufficient without inventorying the vendor's device and all that is on it and creating a baseline configuration for a device that is not owned or managed by the RE. Creating and maintaining such a list has little to no reliability benefit. The point should be to reasonably assure the RE that no malware is present on the device prior to connection a BES Cyber System. As an example, there is no reliability benefit to inventorying that a vendor device has "Siemens WinCC 7" software installed. The benefit to reliability is in scanning that system to see if that copy of WinCC has been compromised by Stuxnet. 6) Under the Guidelines and Technical Basis section, Page 41, under Section: Requirement R4: - consider removing the bullets under "Examples of these devices include…" and simply state "Examples of these devices include, but are not limited to, laptops, desktops, or tablets used for testing, maintenance, configuration changes, and/or vulnerability assessments." 7) Under the Guidelines and Technical Basis section, Page 42, first paragraph at the top of the page - consider having additional guidance on what does NOT constitute a single use. For example – Does use within the same PSP, but for different Cyber Assets at varying impact levels (high & medium) require a new evaluation? Is a new evaluation required prior to use for each instance that a TCA moves from one PSP to another at the same impact level, regardless if the authorized user maintained possession of the TCA, and/or the timeframe for traveling between PSPs is during the same day/week? 8) Under the Guidelines and Technical Basis section, Page 42, section Requirement Part 4.1, No. 1. – consider striking the term "physical proximity" as this is not required by the Standard as written, and would be impossible to prove. Recommend the following change – "This is intended to provide documentation of those personnel authorized to use TCAs." Also – consider striking "unescorted physical access" from the last sentence as there could be instances of personnel with authorized electronic access to the applicable system, but who are not authorized for unescorted physical access to the PSP it is contained within (e.g., periodic vendor support where the vendors are authorized for electronic access to the applicable systems, but are escorted to those systems to perform maintenance and/or troubleshooting.) 9) Under the Guidelines and Technical Basis section, Page 43, under the Section: Requirement Parts 4.2, 4.3, 4.4, 4.5: - the last sentence for the paragraph starting "Part 4.5 requires…" states that "process is to include testing and installing of updated signatures or patterns." This sentence should be struck as it is beyond the scope of the requirement written for CIP-010-2 R4.5. Although it is addressed in CIP-007-6 R3, it is not a requirement in CIP-010-2 R4.5. Southern Company also supports SMUD's comments on this question: 10) SMUD prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of "operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability)" as well as the corresponding Requirement Part 4.6 to "evaluate the Transient Cyber Asset." SMUD believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a "defined acceptable use" for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. SMUD supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. 11) If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state "Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists." As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source requirement part. 12) SMUD is

concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. SMUD does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. SMUD requests guidance be included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review. Southern Company also supports the following EEI comments to the question: CIP-010-2 Requirement R4, Part 4.1: EEI members are concerned with unnecessary administrative burdens created by Part 4.1. For example, Authorization generally applies to users. A user of a Transient Cyber Asset should be authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (CIP-010-2 Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. Southern Company also supports the following GTC comments to the question: In CIP-010-2 Requirement Part 4.4, the SDT proposes language that states that the entity must mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media. The threat for Transient Cyber Assets and Removable Media is not important. The BES Cyber Asset should be protected from detected malicious code on the Transient Cyber Asset or Removable Media. The SDT should consider resolving this issue by eliminating 4.4 and modifying 4.2 and 4.3 as follows: “Use method(s) to detect malicious code on [the Transient Cyber Asset or Removable Media] prior to use on applicable systems and, if detected, do not allow of the use of [the Transient Cyber Asset or Removable Media] until the threat of the detected malicious code to the applicable systems has been mitigated.”
No
Southern Company provides the below comments to the SDT for consideration with regard to new or revised definitions: 1) Removable Media definition should be more specific to the higher risk forms of media, such as USB media, and other diagnostic type devices. 2) Transient Cyber Assets, as written and defined, could include Removable Media as well, which could be interpreted at audit to include additional requirements for Removable Media. The Removable Media definition says that a Cyber Asset is not Removable Media, but the Transient Cyber Asset definition does not exclude it. Southern Company suggests both definitions need to be mutually exclusive for clarity.
Yes
Southern Company fully supports this approach to simply remove the IAC language from the 17 applicable requirements given the development and supporting processes of the Reliability Assurance Initiative (RAI). Southern Company commends NERC on the RAI effort and fully supports it as an alternative to the IAC language and a move away from a zero tolerance approach to compliance.
Yes
Southern Company agrees that the timeframes established in the revised Implementation Plan are reasonable and appropriate.
Yes
Southern Company also supports the following GTC comments to the question: GTC recommends that the SDT clarify the meaning of “associated with” in CIP-002. This clarification comes as a result of the CIP Version 5 Implementation Study and is therefore consistent with the SDT’s SAR. NERC has recently indicated that location is a determinant factor when classifying cyber asset impact. (Reference page 111 from the slides delivered by NERC Compliance at the June CIPC: http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/Presentations%20--%20June%2010-11,%202014.pdf) As such, the SDT should update CIP-002 Attachment 1 Section 2 to indicate that medium impact BES Cyber Assets are those “associated with and located at” the Facilities meeting the criteria of Attachment 1 section 2 in order to clarify the intent of the Standard.

Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
SCE&G agrees with the approach to address the directive concerning Low Impact assets from FERC Order No. 791. With regards to CIP-003-6 R2.4.1, SCE&G believes the SDT must clarify the term "external routable protocol paths". SCE&G proposes the following language to clarify the term: "All external routable bi-directional protocol paths, if any, must be through one or more identified access point(s). With regards to CIP-003 R2.2, SCE&G believes the language "to restrict physical access" included in the requirement is different from what is described in the Technical Guidelines. The Guidelines state that CIP-003 R2.2 can be accomplished using a fence and a lock. Inherently a fence does not "restrict" access; instead, it is a point of demarkation and establishes a boundary. A determined adversary can circumvent a fence in many ways including: climbing over, cutting through, etc. To truly "restrict" access entity's would have to implement additional controls beyond a lock and fence. To align with the controls described in the Technial Guidelines, which SCE&G agrees are adequate for Low Impact Assets, the SDT should consider the following revision: "Implement one or more controls to establish a physical boundary and implement access control(s) to allow access only to legitimate users."
Yes
No
SCE&G believes the SDT needs to reconsider the authorizations and baseline configuration records required under CIP-010 R4.1. Recording such authorizations and configurations will be administratively burdensome for entities. Personnel authorized for access to High and Medium BES Cyber Systems should not require additional authorizations to use Transient Cyber Assets. SCE&G proposes the SDT revise the requirement to require procedures defining the acceptable use of Transient Cyber Assets and a listing of authorized Transient Cyber Assets. Such a list needs to be generic allowing entities to authorize groups of Transient Cyber Assets (e.g. flashdrives issued by the entity). Per NIST 800-53 MA-5, entities should also be allowed to designate personnel with required access permissions to supervise the maintenance actiivities of personnel who do not possess the required access authorizations.
No
SCE&G believes the SDT needs to reconsider the authorizations and baseline configuration records required under CIP-010 R4.1. Recording such authorizations and configurations will be administratively burdensome for entities. Personnel authorized for access to High and Medium BES Cyber Systems should not require additional authorizations to use Transient Cyber Assets. SCE&G proposes the SDT revise the requirement to require procedures defining the acceptable use of Transient Cyber Assets and a listing of authorized Transient Cyber Assets. Such a list needs to be generic allowing entities to authorize groups of Transient Cyber Assets (e.g. flashdrives issued by the entity). Per NIST 800-53 MA-5, entities should also be allowed to designate personnel with required access permissions to supervise the maintenance actiivities of personnel who do not possess the required access authorizations.
No
NERC has advised that the IAC language will be replaced by the RAI process. Final ballot on the removal of the IAC language must not occur until RAI is approved. It is unreasonable to ask entities to remove such language without an approved alternate process to take its place.
No
Implementation has been negatively impacted by the everchanging state of the CIP V5 standards. To ensure cost-effective and appropriate implementation for their customers and shareholders, entities do not want to extensively begin implementation until the target stops moving. As is now the case, entities have lost precious months on the already time constrained implementation timeframe. This, in addition to the delay in the much needed Transition Guidance from the NERC Implementation Study, must be taken into consideration by NERC/FERC. Steady-state standards and clear transition guidance are essential to entities being able to successfully implement the new CIP

standards. SCE&G proposes that all standard implementation start dates be revised to reflect the completion of the CIP V6 revisions and the issuance of the Transition Guidance from NERC.
No
No
Individual
Joshua Andersen
Salt River Project
No
The Requirements proposed in 2.1, 2.2 and 2.3 provide appropriate controls for Low Impact Cyber Systems. However, the “external routable protocol paths” language in Requirement 2.4 requires entities with Low Impact Cyber Systems to provide and comply with “some form of electronic security perimeter,” regardless of risk to the Bulk Power System/Bulk Electric System. Compliance to this requirement would be excessive given the risk associated with Low Impact rated BES Cyber Systems. Additionally, entities would be required to identify, maintain and comply with “some form of electronic security perimeter” (ESP) for Low Impact rated BES Cyber Systems, yet additional revisions state that “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” This is contradictive at best and should be clarified. Recommend language changes to address only Low Impact Systems which have direct internet access. Recommend adding language which assesses risk to Low Impact BES Cyber Systems with “external routable protocol paths.”
Yes
No
CIP-010-6 R4.1.4 requires the Entity to “identify and document the Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).” And in 4.6, the Entity is required to “Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4.” For entities that depend on vendors and contract support personnel to maintain the Reliability of the Bulk Electric System, this becomes a great administrative challenge. This requirement becomes dependent upon the number of Transient Devices, the number of vendors, contractors or support personnel, and the type and variance of Transient Cyber Assets and tools used to perform their job duties. The challenge in requiring a baseline of firmware alone far exceeds the vulnerably and risk to the BES Cyber Asset. Recommend changing the language in requirements R4.1.4 and R4.6 to address Entity owned-maintained Transient Devices separately from Vendor or Contracted Support owned-maintained Transient Devices. This allows entities to reasonably develop and implement Administrative and Technical Security Controls for Transient Devices based on risk, yet monitored from a compliance standpoint. Recommend language changes to require “the implementation of a Transient Device Security Baseline for Entity and Vendor/Contracted Support Transient Devices.” This allows Entities to implement controls yet maintain the flexibility to address multiple device types and functions. This also allows Entities and their vendors or contracted support personnel to implement Administrative and Technical controls of Transient Devices based on risk. Recommend language changes to require sampling of Transient Devices Security Baseline. This allows Entities a mechanism for monitoring both Entity and Vendor/Contracted Support personnel owned-maintained Transient Devices. Recommend language changes to require a security policy for Transient Devices which includes a requirement for Transient Devices with direct access to BES Cyber Systems. This allows Entities to establish and implement Administrative Controls for Transient Devices.
Yes
Yes
No

Recommend changing the Implementation Plan time schedule to fall after the CIP Version 5 standards implementation dates.
No
No
Group
Associated Electric Cooperative, Inc. - JRO00088
Phil Hart
No
AECI agrees with NRECA comments. Regarding 2.3.1 - Escorted should be removed. Typically, these facilities are smaller work environments that can manage appropriate access to visitors via a policy without the need to require escort. Regarding 2.4.2 - This requirement should be removed or reduced to not include inbound and outbound access permissions, and more importantly remove the reason for granting access. This requirement is a very specific control that FERC specifically stated was not needed. Although this is common practice for most entities, the compliance burden created to prepare for audit exceeds the benefit gained in reliability. Management of all firewall rules at all low impact facilities is a tremendous effort for small entities, and the largest gain in reliability is realized with the creation of processes to address these items, not specifically listing each. If requirement 2.4 stated "Implement one or more documented processes that collectively address the following…" and it is understood that entities would only be required to have implemented procedures that consider these items, and not specifically list them, then AECI would argue this more accurately represents the FERC order by creating a requirement that could be used to evaluate the sufficiency of a program without developing specific controls such as this draft currently has. The corresponding measure would also need to include language that allows for flexibility of procedures to not include every specific inbound and outbound permission rule. Entities with sufficient resources and capability could include specific listings of these rules to demonstrate exceptional compliance, however those without the means would not be held liable for over-specific controls on facilities that have no impact to the BES.
No
AECI agrees with NRECA comments.
No
AECI agrees with NRECA comments.
No
AECI agrees with NRECA comments.
Yes
AECI agrees with NRECA comments.
No
AECI agrees with NRECA comments. It would be very advantageous if industry was allowed to triage compliance on LIAs, similar to the FAC-008 alert. More significant impact LIA facilities would be addressed first in implementation plans while less significant facilities would receive additional time to become compliant.
Yes
AECI agrees with NRECA comments.
Individual
David Revill
Georgia Transmission Corporation
No
We are concerned that by borrowing language from Medium Impact requirements, the SDT has introduced a substantial increase in administrative overhead to comply with the standard without an equivalent increase in security. Specifically, maintaining the documentation of justifications for every

firewall rule results in a significant amount of man-hours devoted to compliance and not to improving the security of the low impact assets. We instead recommend the following language for CIP-003 R2: R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3 (assets containing low impact BES Cyber Systems), shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2.1 Review and obtain CIP Senior Manager approval at least once every 15 calendar months for a cyber security policy that addresses CIP-003-5, Requirement R2, Part 2.2. 2.2 The Responsible Entity shall implement one or more documented processes that collectively address the following topics: 2.2.1 Operational or procedural control(s) that restrict physical access to low impact BES Cyber Systems; 2.2.2 Access control(s) to restrict electronic access to low impact BES Cyber Systems via the asset's external routable protocol connections and Dial-up Connectivity, if any; 2.2.3 Cyber security incident response including conditions for activation of the response plan(s), roles and responsibilities of responders, and determination if an identified Cyber Security Incident is a Reportable Cyber Security Incident with notification of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law; and 2.2.4 Security awareness for the Responsible Entity's personnel that, at least once each calendar quarter, reinforces cyber security practices. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.
Yes
Yes
No
Similar to its comments on Low Impact, we disagree with simply borrowing requirement language from Medium impact requirements for Transient devices. In this case, we believe that the SDT has provided unnecessary administrative overhead and introduced constructs that are not ideal for transient devices. Requirement part 4.1 requires authorization, but provides little security benefit. In particular, the SDT proposes that defined acceptable be authorized. Almost all companies have an existing acceptable use policy. However, it seems this may not be the intent of the SDT. The SDT should be clearer about the intent so that it is simply requiring entities to create lists and perform administrative exercises in order to prove compliance. In requirement part 4.4, the SDT proposes language that says that the entity must mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media. The threat for Transient Cyber Assets and Removable Media is not important. It is the BES Cyber Asset that should be protected from detected malicious code on the Transient Cyber Asset or Removable Media. The SDT could resolve this issue by eliminating 4.4 and modifying 4.2 and 4.3 as follows: "Use method(s) to detect malicious code on [the Transient Cyber Asset or Removable Media] prior to use on applicable systems and if detected, do not use this [Transient Cyber Asset or Removable Media] until the threat of the detected malicious code to the applicable systems has been mitigated."
Yes
Yes
No
Yes
We recommend that the SDT clarify the meaning of "associated with" in CIP-002. This clarification comes as a result of the CIP version 5 implementation study and is therefore consistent with the SDT's SAR. NERC has recently indicated that location is a determinant factor when classifying cyber asset impact. (Reference page 111 from the slides delivered by NERC Compliance at the June CIPC: http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/Presentations%20--%20June%2010-11,%202014.pdf) As such, the SDT should update CIP-002 Attachment 1 Section 2 to indicate that medium impact Cyber Assets are those "associated with and located at" the Facilities meeting the criteria of Attachment 1 section 2 in order to clarify the intent of the standard.
Individual

Nathan Mitchell
American Public Power Association (APPA)
No
APPA agrees that some of the changes the SDT has made in the draft standards address the recommendation in order 791 the Commission “defining with greater specificity the processes that responsible entities must have for Low Impact facilities under CIP-003-5.” However, APPA believes the SDT has gone too far in certain aspects of this specificity to include requirements that impose compliance costs that exceed the reliability benefit to the BES. Cost of compliance with CIP standards must be in line with the risk of malicious actions that could cause instability, uncontrolled separation or cascading failures. The thresholds for the high and medium impact categories were selected to ensure that specific security controls are in place in facilities that can cause instability, uncontrolled separation or cascading failures. The programmatic controls for low impact facilities were designed to ensure security policies and procedures covered all BES Cyber Systems. In particular, APPA believes the SDT has not taken into consideration this cost to risk evaluation in the development of the new requirements in CIP-003 R2 Part 2.3. The new requirement in Part 2.3.1 which requires escorted access for visitors will impose a significant burden without a commensurate reduction in cyber security risk for reliable operation of the BES. APPA believes the cost of developing and implementing a documented process for escorted visitor access for Control Centers that control multiple facilities by voice instruction only is out of line with the risk to reliable operation of the BES. For example, APPA members report that CMEP personnel rely on FAQs developed for previous versions of CIP standards to conclude that Control Centers that “control” remote Facilities through voice commands only are subject to the CIP standards. See NERC link: http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf (Question 9). If it was the intent of the SDT to limit the scope of 2.3.1 to Control Centers with capability to control multiple facilities automatically or remotely, this must be stated specifically in the standard. Ultimately, APPA recommends that the SDT remove 2.3.1 since this requirement would not significantly reduce the risk of instability, uncontrolled separation or cascading failures on the BES. The intent of segmenting out Low Impact facilities was to assure that programmatic controls were in place for those facilities that had “Low Impact” on the BES. The compliance burden on these systems must be in proportion to its impact on the BES. APPA recommends that the SDT evaluate compliance costs in any changes they make to the revised standards prior to the final ballot.
Yes
APPA appreciates the SDT providing flexibility to entities in complying with R1 Part 1.10. Having multiple options for controls when physical access restrictions are not possible gives entities an opportunity to select the solution that works for each specific situation. Industry has commented that encryption of data as a sole solution may reduce reliability by adding complexity to the systems and introducing latency to data flow that will not work in a relay control environment. If the SDT removes this flexibility or expands the applicability in future drafts APPA will need to reevaluate its support for the communications controls.
No
APPA supports the comments of SMUD on this question
No
APPA supports the comments of SMUD on this question
Yes
APPA supports the removal of the Identify, Assess, and Correct (IAC) language from the 17 requirements. APPA encourages the SDT to provide guidance to NERC staff on the development of the proposed RSAWs. This guidance will give regional auditors insight to the intent of the SDT in drafting the standards and the reliability outcomes. APPA members would appreciate a commitment from NERC staff to timely complete development and publish details of the RAI program to give industry an indication of the proposed enforcement discretion program. This may give them more confidence to cast an affirmative vote for these changes in the final ballot.
No
If the draft requirements for Low Impact Control Centers remain then a new implementation date for these requirements must be considered. APPA recommends a 1 year extension to April 1, 2018 for Low Impact Control Centers since entities will need time to budget and implement security controls

in addition to developing compliance plans. Due to the uncertainty created by this revision process and not knowing what the Commission will order or when the final rule will be issued, the SDT needs to revise the implementation options for CIP-003-6 R2. APPA recommends modifying the implementation plan for CIP-003-6 to become enforceable 2 years after Commission approval or April 1, 2017, whichever is later.
Yes
The SDT proposals will increase the compliance burden by adding requirements to the Low Impact sections. APPA urges NERC to survey registered entities, especially small entities, to estimate the real compliance cost of CIP V6 Revisions before the standards are submitted to FERC for approval. APPA in its comments to the Commission in the CIP V5 NOPR asked that FERC require NERC to do this survey. However in P261 of the Final Rule FERC stated, “To the extent that entities provide NERC with such information, we encourage NERC to submit the cost data along with the associated new or revised Reliability Standards requirements.”
Individual
Nicholas Lauriat
Network & Security Technologies
No
Proposed "Transient Cyber Asset & Removable Media Protection" requirements 4.3 and 4.6 of CIP-010-2 compel malicious code detection (4.3) and an evaluation of current configurations against a previously established baseline (4.6) “prior to use.” These two requirements are unacceptably ambiguous by virtue of the fact a “use” is not defined within the language of any CIP V5 requirement. The SDT has attempted to define “use" in the Guidelines and Technical Basis section as follows: "For purposes of this standard, ‘use' is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use.” However, as NERC representatives often point out, guidelines are non-binding. Moreover, N&ST believes the suggested definition of “use,” if widely adopted as an audit benchmark, could create unacceptable and counter-productive administrative and compliance burdens for Responsible Entities. If a technician used a laptop to test BES Cyber Systems at a Control Center and then drove directly to the backup Control Center, the Responsible Entity would be at risk of being found non-compliant with R4.6 unless the prescribed evaluation was performed before the technician used that same laptop to perform similar BES Cyber System testing. N&ST appreciates the importance of minimizing the risk of introducing malicious code to BES Cyber Systems via transient devices and removable media. However, N&ST believes these requirements should be modified to avoid a negative impact on BES operations. One option the SDT might consider is to make R4.3 and R4.6 time-based requirements (e.g. every 30-60 days), with the additional provision of requiring R4.3 malicious code detection and R4.6 evaluations to be performed “prior to use” for any transient devices or removable media that have been used for any purpose other than for interaction with applicable systems.
Individual
Thomas Standifur
Austin Energy
No
The addition of more objective criteria for Low impact BES Cyber System Requirements within CIP-003-6, R2, breaks one of the prime objectives defined when CIP version 5 was being developed that each of the Standards could stand on its own. Entities with Low “and” either Medium or High Cyber BES Cyber Systems, it would be necessary that CIP-003 “always” be referenced when any of the

requirements in CIP-004-6 through CIP-011-2 for the Medium and High Impact BES Cyber Systems are being designed and implemented, since dependencies are always possible between Cyber Systems part of any impact category. The inclusion of these objective requirements with a unique table in CIP-003-6 result in Standards language inconsistencies that creates confusion and additional compliance risks. A new definition is now needed for CIP-003-6, R2, Requirement Part 2.4 for the phrase “external routable protocol paths” to ensure that entities and auditors clearly understand the differences between that phrase and the defined term External Routable Connectivity. This would avoid duplicating the confusion seen in earlier versions of the CIP Standards, such as the CIP-001 confusion between Facilities and facilities. The phrase “external routable protocol paths” may create a similar interpretation risk.
Yes
No
AE prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of “operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability) as well as the corresponding Requirement Part 4.6 to “evaluate the Transient Cyber Asset.” AE believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a “defined acceptable use” for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. AE supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state “Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists.” As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source requirement part. AE is concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. AE does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. AE requests guidance be included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review.
Yes
Yes
Yes
No
No
Individual
Michelle D'Antuono
Ingleside Cogeneration, LP
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
No
NRECA understands that the approach to add greater specificity and auditability to the required processes in CIP-003 R2 can fulfill the FERC directive in Order No. 791. However, NRECA has

concerns with the requirements in the current proposed draft. From a policy level, we are concerned that the revisions go beyond what the FERC directive required and that the distinction between low and medium impact BES Cyber Systems is becoming less and less clear. Additionally, the current proposed revisions are increasing the financial, compliance and operational burdens on entities for low impacts beyond the benefits it will provide to BES security and reliability. The emphasis, burden and investment of resources for entities must continue to focus on their finite resources on addressing the most impactful first (High and Medium), and then the least impactful (Low). NRECA believes that the primary focus on cyber security must remain with the Medium and High Impact classified facilities. By definition, Low Impact facilities are categorized as low because failure or degradation of those assets have minimal to no impact on BES reliability. The financial, compliance and operational burdens must be commensurate with the risk to the reliability of the BES, which specifically applies to preventing instability, cascading or uncontrolled separation of the BES. It is difficult to see how the CIP-003 R2 revisions and additions could help to limit BES instability, cascading or uncontrolled separation. NRECA requests that the SDT demonstrate how all changes to CIP-003 R2 will contribute to preventing instability, cascading or uncontrolled separation of the BES. NRECA is concerned that by borrowing language from Medium Impact requirements, the SDT has introduced a substantial increase in administrative overhead – staffing and financial -- to comply with the standard without a commensurate impact on BES reliability and security. Specifically, maintaining the documentation of justifications for every firewall rule results in a significant amount of man-hours devoted to compliance and not to improving the reliability and security of the low impact assets. NRECA instead recommends the following language for CIP-003 R2: R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3 (assets containing low impact BES Cyber Systems), shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2.1 Review and obtain CIP Senior Manager approval at least once every 15 calendar months for a cyber security policy that addresses CIP-003-5, Requirement R2, Part 2.2. 2.2 The Responsible Entity shall implement one or more documented processes that collectively address the following topics: 2.2.1 Operational or procedural control(s) that restrict physical access to low impact BES Cyber Systems; 2.2.2 Access control(s) to restrict electronic access to low impact BES Cyber Systems via the asset's external routable protocol connections and Dial-up Connectivity, if any; 2.2.3 Cyber security incident response including conditions for activation of the response plan(s), roles and responsibilities of responders, and determination if an identified Cyber Security Incident is a Reportable Cyber Security Incident with notification of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law; and 2.2.4 Security awareness for the Responsible Entity's personnel that, at least once each calendar quarter, reinforces cyber security practices. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Mandating specific controls could have the undesirable consequence of stunting the development of the range of controls necessary to protect the diversity of Low Impact assets. Entities should be afforded discretion to utilize their experience and expertise to develop controls that protect their assets commensurate with the BES reliability risk posed. At this juncture, a one-size-fits-all approach that imposes greater obligations on Low Impact BES Cyber Systems would simply increase costs and burden, without commensurate benefits, to both the Registered Entities and the Regional Entities charged with ensuring compliance with the CIP standards. NRECA supports the SDT position that entities subject to the Low Impact BES Cyber System requirements in CIP-003-5 R2 to keep an inventory or list to help ensure that they have properly identified and categorized the location of its BES Cyber Systems. However, the currently proposed requirements all but require the development of such a list. NRECA request that the SDT revise the requirements so that such a list is not indirectly or directly required. Requiring entities to maintain a discrete list of Low Impact BES Cyber Systems, as opposed to the location of such assets, will involve considerably more time and cost, again without any commensurate benefit to BES reliability and security. While not the work of the SDT, RAI and the RSAWs are companion pieces to the CIP V5 standard revisions. Unfortunately, the initial draft RSAWs don't provide the needed clarity or relief from the zero defect compliance expectation. NRECA encourages NERC to continue their work and collaboration with the SDT and to post revised RSAWs with next comment and ballot period for CIP V5 revisions. Regarding RAI, NRECA recommends that NERC use the requirements on Low Impact assets to demonstrate how RAI can alleviate the compliance concerns and create a reasonable approach to compliance. This may be essential for the passage of revised requirements on Low Impact assets. Additionally, if RAI is not adequately explained and clearly understood before the next comment and ballot period, NRECA believes that ballots for the CIP V5 revisions may be

negatively impacted. Some “affirmative” ballots may change to “negative” without a better understanding of RAI and how it relates to the CIP V5 revisions.
Yes
NRECA views Requirement CIP-007 R1.2, as only specifying how to be compliant with other requirements within the suite of CIP Standards. Adding duplicative requirements only increases the compliance burden and audit confusion, without commensurate value to increased BES security and reliability. NRECA requests the SDT review this issue and remove duplicative requirements from the CIP standards. NRECA is concerned that the new and undefined term of “nonprogrammable communication components.” We request that the SDT provide more clarity around the meaning of the this term. NRECA requests additional guidance related to CIP-006 R1.10 on what constitutes adequate physical protection of connectors joining separate conduit sections. This is needed to minimize confusion at audit.
No
NRECA recommends the SDT remove new CIP-010 R4.1.4. Defining users, locations and acceptable use of these devices should be sufficient to protect these devices from unauthorized or harmful use. This requirement expands in R4.6 and R4.7 and becomes extremely difficult to manage. A detailed listing of all software and hardware is not necessary to fulfill requirements R4.6 and R4.7. An effective change management procedure coupled with documents required in R4.1.1 R4.1.2 and R4.1.3 will allow for objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity’s protections without the need for a prescriptive list. Further, compliance with R4.6 and R4.7 will likely be met through the use of software whitelisting, not documentation. A documented list of operating system, firmware, and software on transient devices is not needed for such an implementation and provides no benefit to BES reliability and security which should be focused on preventing instability, cascading and uncontrolled separation of the BES.
No
NRECA believes the Transient Cyber Asset definition language is overly broad. Using "directly connected" would apply to any programmable device, whereas the focus should be towards devices that can infect, alter, or transfer files to a BES Cyber Asset. Recommended language for a revised definition is as follows:: Transient Cyber Asset: A Cyber Asset directly connected, and able to infect, alter, or transfer files to BES Cyber Assets, for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. NRECA disagrees with the SDT’s borrowing requirement language from Medium impact requirements for Transient devices. In this case, we believe that the SDT has provided unnecessary administrative overhead and introduced constructs that are not ideal for transient devices. Requirement part 4.1 requires authorization, but provides little security benefit. In particular, the SDT proposes that “defined acceptable use” be authorized. Almost all companies have an existing acceptable use policy. However, it seems this may not be the intent of the SDT. The SDT should be clearer about the intent so that it is not simply requiring entities to create lists and perform administrative exercises in order to prove compliance. In requirement part 4.4, the SDT proposes language that says the entity must mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media. The threat for Transient Cyber Assets and Removable Media is not important. It is the BES Cyber Asset that should be protected from detected malicious code on the Transient Cyber Asset or Removable Media. The SDT could resolve this issue by eliminating 4.4 and modifying 4.2 and 4.3 as follows: “Use method(s) to detect malicious code on [the Transient Cyber Asset or Removable Media] prior to use on applicable systems and if detected, do not use this [Transient Cyber Asset or Removable Media] until the threat of the detected malicious code to the applicable systems has been mitigated.”
Yes
NRECA believes removal of IAC language clarifies those requirements and what is expected during audit; but without RAI adequately explained and clearly understood before the next comment and ballot period, NRECA believes that ballots for the CIP V5 revisions may be negatively impacted. Some “affirmative” ballots may change to “negative” without a better understanding of RAI and how it relates to the CIP V5 revisions.
No

NRECA has several significant concerns with the proposed Implementation Plan (IP). First, it appears that the IP is posted only for comment, but not for ballot. NRECA asserts that this potentially violates the NERC Standards Process Manual (SPM). While there are many references in the SPM requiring the IP to be balloted, NRECA directs SDT and NERC attention to SPM Sections 4.4.3, 4.6, 4.8, 4.16 for provisions that clearly require the IP to be balloted. In this current formal comment and ballot period, entities can only submit comments on IP – there is no provision or ability to cast a ballot on the IP as the SPM requires. NRECA requests that this potential SPM violation be addressed expeditiously as possible to ensure the CIP V5 revisions are developed in clear compliance with the FERC approved NERC SPM. NRECA believes the proposed IP does not adequately provide enough additional time to comply with the currently proposed revisions and new requirements to the CIP V5 standards. For those revised and new requirements, NRECA requests additional time be included in the IP that matches the time entities were originally provided upon FERC's approval of CIP V5. If the original amount of time that was provided for CIP V5 was adequate then, it should also be adequate for revised or new requirements for the CIP V5 revisions. This is especially critical for the new requirements in CIP-003-6 R2. NRECA also requests that the SDT consider using the same additional time for compliance for all revised or new requirements under the current CIP V5 revision project. One of NRECA's members estimates that its implementation burden for the currently proposed CIP-003-6 R2.4.2 will take over 4000 hours initially and 2000 hours annually. Depending on the final requirements, these estimates could increase.

Yes

NRECA supports addressing FERC's four directives in the current project. Industry needs stability, closure, and a steady state of CIP standards so that industry can comply with a non-moving target of requirements. NRECA supports the RAI concept, but is seeking greater understanding of and informative experience with RAI. For NRECA and its members, filling this gap may be essential for the passage of revised requirements, in particular for Low Impact assets. Low Impact asset requirements are ideal to demonstrate how RAI can alleviate the compliance concerns and create a reasonable approach to compliance.

Group

Bonneville Power Administration

Andrea Jessup

No

Although the proposed controls and objectives are clear as written, BPA believes they are insufficient to adequately provide protection of the BES. If the low impact assets represent the majority of the BES, the proposed NERC CIP standards should address risk due to aggregated impact and reduce the extremely large attack surface. BPA suggests the requirement language should include an annual assessment of BES LIA to baseline and monitor their security status. In addition, BPA believes the LIA requirements should be distributed throughout each of the proposed standards (CIP-002 through CIP-014.)

No

Although the proposed scope is clear and auditable, BPA believes the control coverage is insufficient to provide adequately assured protection of the BES. If the low impact assets represent the majority of the BES, and non-routable communications are no longer considered "safe," the proposed NERC CIP standards should address risks related to all open system interconnection layers (physical to application.) Attacks against communication networks have evolved where protocol types are no longer relevant.

No

While BPA agrees that CIP-010 R4 addresses the risks related to High and Medium impact assets, the proposed requirement language should also address Low Impact Assets. In addition, BPA suggests requirement language should be added to include implementation of Transient Device baselines, with periodic sampling, for entity and vendor managed devices. Entities may also consider removing direct-access to BES assets by Transient Devices (e.g. jumpbox, proxy, etc.) Furthermore, standards addressing transient devices must acknowledge the nature of these devices and the fact that the responsible entity does not always exercise continuing controls over these devices. Policies, procedures, and technological solutions must focus on transient devices at the time of connection

and on controlling the interfaces to the system rather than attempting to exercise continuous control over control over a device of a transient nature.
Yes
No
BPA supports the removal of the IAC language and the move away from “zero defect” requirements. However, BPA believes the lack of clearly defined measures results in inconsistent audit approaches and findings. In addition, BPA expects the RAI will be fully vetted publicly.
Yes
The additional timelines are sufficient. However, BPA suggests that all CIP Version 5/6 requirements become effective on this revised date to avoid confusion, with the exception of Low assets which are afforded a minimum of an additional 12 months before the initial compliance date.
No
No
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
Yes
No
CIP-006 R1.10: “monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection…” When does “detection” actually occur? A 15 minute window for notification is typically not sufficient to respond to an automated alert during regular business hours, and would be impossible after hours. The last bullet of R1.10, “an equally effective logical protection” is ambiguous. Who/what would determine the effectiveness of logical protection other than the two previous bullets? Tri-State suggests removing this bullet. Tri-State believes that there is still a need to define what a communication network is. This was ordered by FERC and we do not agree that this has been clarified in the current draft.
Yes
How does the SDT anticipate that RE’s enforce/assess Transient Cyber Assets and Removable Media that are owned and maintained by consultant services? CIP-004 R1 should read R2 in the question above. For R2.1.9, it reads better as “…and interoperability with other Cyber Assets, including Transient Cyber Assets and Removable Media.”
Yes
No
The FERC Order “directed NERC to remove the “identify, assess, and correct” language or to propose modifications that addressed the Commission’s concerns about the ambiguity and enforceability of that language.” Tri-State feels that the IAC language is helpful and the removal solution attempted was overly complicated and left gaps that were not all adequately addressed. The removal of identify, assess, and correct also diminishes the value of the standards. It would have been much simpler to have “proposed modifications that addressed the Commission’s concerns about the ambiguity and enforceability of that language.” The easiest solution is to define “identify, assess, and correct” as one defined term rather than as three separate words. Tri-State also recommends that the term “deficiencies” when referenced with IAC language be changed to “possible violations” as defined in NERC’s Compliance Monitoring and Enforcement Program to remove ambiguity.
Yes
No

No
Individual
Bill Temple
Northeast Utilities
No
In an effort to differentiate the compliance responsibilities for entities between Medium and Low Impact Assets, the SDT has in effect ended up creating a greater burden on entities to create, manage and define programs that meet compliance. The requirements of this revision are inconsistent and overly complex. Examples include but may not be limited to; ¬ Ambiguous and inconsistent terms “External Routable Paths” versus “External Routable Connectivity”. ¬ More restrictive requirements for Low Impact Assets. ¬ Inconsistent Testing Time frames. ¬ Instances where there was a Failure to extend implementation Time frame beyond the original version 5 effective compliance date.
Yes
Please expand on the expectations for meeting this requirement with regard to "patch panels". 1. If the Cyber Assets in the ESP are meeting the requirements by disabling unneeded ports on the device, is there any action needed on the patch panel? 2. The patch panel may have connectors that are not used or may be connected to ports that are disabled. Is signage or tamper tape truly required on the patch panel in that situation?
No
Please expound upon the “CAUTION” statement in the Guidelines and Technical Basis. For example, would it be permissible to have a Transient Cyber Asset use a secure wireless network to only access a secured network drive containing relay configuration data. For Transient Cyber Assets, please consider adding a statement in the Guidelines and Technical Basis from CIP-007-5 R3 “If a specific Transient Cyber Asset has no updateable software and its executing code cannot be altered, then that Transient Cyber Asset is considered to have its own internal method of deterring malicious code.” With the proliferation of IEC61850 substations, test equipment with proprietary software and executing code are commonly used. Please provide examples where a transient cyber asset had wireless enabled such that the transient cyber asset was not an electronic access point.
Yes
Yes
No
CIP-003-6 R2 compliance enforcement date needs to change from the version 5 compliance enforcement date. (April 1st 2017). Recommend Nine months after the compliance enforcement date of version 5 (February 1st 2018
No
Individual
Jen Fiegel
Oncor Electric Delivery Company LLC
No
Oncor supports comments submitted by EEI and Southern Company
Yes
Oncor supports comments submitted by EEI and Southern Company
No
Oncor supports comments submitted by EEI and Southern Company with the following additional comments: CIP-010-2 R4.1 – Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. This requirement places a lot of overhead to maintain lists

or some form of documentation that documents for each transient cyber asset that connects to a Medium Impact BES Cyber System and tying it to some defined initial use time to show compliance. Most of the assets in Medium Impact BES Cyber systems are assets in substations that don't have communication external to the substation therefore the stated "initial use" would be hard to determine let alone document to the level of accuracy needed to establish compliance. Additionally, this burdensome requirement of creating and maintaining such lists adds little or no benefit to reliability or security. Oncor's requests consideration that requirement 4.1 not be applicable to Medium Impact BES Cyber Systems. A better alternative would be authorized users whose transient devices meet 4.1.4 compliance of having pre-authorized operating system, firmware, and intentionally installed software.
No
Oncor supports comments submitted by EEI and Southern Company
Yes
Oncor supports comments submitted by EEI and Southern Company
No
Oncor supports comments submitted by EEI
No
Yes
Oncor supports comments submitted by EEI
Individual
Judy VanDeWoestyne
MidAmerican Energy Company
No
Limit the applicability for dispersed generation to the point where those resources aggregate to greater than 75 MVA to a common point of interconnection at 100 kV or above and not at an individual turbine, inverter or unit level in the CIP-003-6 Applicability section similar to PRC-005. This applicability change would apply only in CIP-003-6 standard for the low impact asset requirements. See comments on question 8. // Table titles in other standards reflect the requirements not the applicability. We recommend changing the table title for consistency to: "CIP-003-6 Policies, Processes, Plans and Programs." // Background Section 6: With the addition of the tables, the Introduction Background Section 6 should include a paragraph referencing the tables and the "Applicable Systems" Columns in Tables section that is included in the Background section for other standards. ***The paragraph for CIP-003-6 Background Section 6 would be: "Requirement R2 opens with, "Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 –Policies, Processes, Plans and Programs." The referenced table requires the applicable items in the procedures for the requirement's common subject matter." Insert the Applicable Systems boiler plate from other CIP standards into the Background Section 6 for CIP-003-6 with regard to Requirement R2. // In R2: Add back: "for its assets identified in CIP-002-5.1 Requirement R1.3" in CIP-003-6 R2 for clarification. ***Revise the requirement to: "Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Policies, Processes, Plans and Programs. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required." // Requirement R2, Part 2.1 – An entity may not have a low impact BES Cyber System at a Control Center (R2.3) and therefore R2, Part 2.3 is not applicable. ***Revise the requirement text to: "that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 -2.6." // Requirement R2, Subpart 2.4.2 - Remove "by default" as it implies the use of a firewall, which limits access control options. For example, an entity could use access control lists on a router or switch to provide security for traffic control. However, routers and switches do not do this by default. This will allow entities more options on how to accomplish traffic control. Include allowance for access permission reasons by individual or group in the requirement. ***Revise requirement R2.4.2 to: "For each identified access point, if any, require inbound and outbound access permissions and deny all other

access. Document access permission reasons individually or by group." // Requirement R2, Part 2.6 - The specificity of what must be covered and tracking two time periods is more prescriptive than the requirements for medium and high impact BES Cyber Systems and is not commensurate with the risk. The proposed revision uses language from the medium/high impact requirement (CIP-004-R1.1) with the time period adjusted to once every 15 calendar months to differentiate for the lower risk. Cyber security awareness can be addressed during annual training for employees and contractors in addition to other ongoing cyber security awareness communications. Remove references to other subpart requirements as all subparts may not apply to all entities. ***Revise requirement to: "Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months." // Guidelines and technical basis – Clarify the drawings by more specifically identifying the external routable path(s). It appears that users of the guidelines are to infer the business network is a separate external routable protocol path. Please reconsider the drawings.
Yes
We agree with the approach to address protections for nonprogrammable components of communication networks. // We have concerns regarding the removal of the "identify, assess and correct" language. See comments on question 5. // We recommend an addition to the guidelines and technical basis for CIP-006-6 R1.10 to capture FERC's clarification that entities are not expected to enforce this requirement on third party nonprogrammable components that are out of the entities' control.
No
No changes are needed for the malicious code and signatures/patterns Parts 4.2, 4.3, 4.4 and 4.5. // We do not agree with Part 4.1. FERC's Order 791 noted the approach to addressing the risks associated with transient devices should be done without imposing unduly burdensome requirements on responsible entities. The controls in Parts 4.1 should be revised to reduce burden. Subpart 4.1.1 should not require users to be authorized for the Transient Cyber Asset if users are already authorized for the applicable systems. Duplicate authorization would be unduly burdensome. Subpart 4.1.2 and 4.1.4 are unduly burdensome by requiring the additional obligation of authorization for locations and software. FERC's directive can be addressed by documenting the locations and software, without requiring authorization. Subpart 4.1.3 and 4.1.4 require documenting defined acceptable use, operating systems or firmware, which is exceeds FERC's directive. Part 4.6 references Subpart 4.1.4. // We recommend revising Part 4.1 to only address user authorization. We recommend a separate part for documenting locations. We recommend a separate part for documenting software. Retain the applicable systems in 4.1 for the revised 4.1 and the two new Parts (High and Medium Impact and associated PCA.) *** Recommended text *** Part 4.1 – "Authorize, except for CIP Exceptional Circumstances, users individually or by group/role for electronic access to the Transient Cyber Asset when it is not required to authorize users for electronic access to the applicable systems to which the user is connecting. Authorization is based on need, as determined by the Responsible Entity. (When users are already authorized for electronic access to the applicable systems the user is connecting to, additional authorizations for the Transient Cyber Asset are not required.) OR Designate organizational personnel with required electronic access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required electronic access authorizations." This is from NIST 800-53 Control MA-5, which provides an option for escorted electronic access. FERC Order 791 paragraph 136 refers to the MA and MP NIST controls. ***Recommended text Part 4.X – "Document locations of applicable systems, individually or by group/role where the Transient Cyber Assets can be directly connected to applicable systems. Document if the Transient Cyber Asset may be directly connected to non-applicable systems. A list of non-BES locations is not required." (Separate Transient Cyber Assets are not required for different BES impact levels or non-BES and are not practical for substations.) *** Recommended text Part 4.Y – "Document software installed on Transient Cyber Assets (per Cyber Asset capability.)" // In Part 4.6, revise the reference to Subpart 4.1.4 to the new Part 4.Y. // We propose a few changes for Part 4.7. ***Revise the requirement to: "Evaluate Transient Cyber Assets, within 35 calendar days prior to use, for applicable security patches and take one of the following actions: (bullet) Apply the applicable patches; or (next bullet) Create a mitigation plan; or (next bullet) Revise an existing mitigation plan. // The goal is to protect the applicable system(s) to which the Transient Cyber Asset will be connected. To clarify this, the structure of the applicable systems column should be revised to follow the model used for PACS in CIP-006-5 R1.1. For

example, ***revise applicability to: “Transient Cyber Assets directly connected to (bullet) High Impact BES Cyber Systems and their associated PCA, (next bullet) Medium Impact BES Cyber Systems and their associated PCA”. If this change is made the guidance won’t need to be revised, Requirement R4: This requirement applies to any transient devices...” // Guidance also suggests, “It may be reasonable to have separate Transient Cyber Assets for each impact level.” It is not reasonable. It would be cost-prohibitive and complicated to track. // “Prior to use” for every transient device every time the device is moved from one ESP (or PSP) to another is not practical for the associated level of risk.
No
We agree with the revised definitions and with the new definition for Transient Cyber Assets. However, although the definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to, the definition for Removable Media does not name what Removable Media are connected to. Also, the final sentence sounds backwards. We recommend the following ***revised definition: “Removable Media: Portable media, connected for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
No
We agree with the standard drafting team’s approach to remove the “identify, assess and correct” language and the concept of compliance exceptions to address the resulting gap. However, we are concerned compliance exceptions have not been implemented for all entities. Similar concerns were expressed at the MRC pre-meeting on July 16. NERC can support Standard Drafting Team efforts by implementing compliance exceptions prior to the second or final ballot.
No
The implementation plan should provide for skipping CIP version 5 in the scenario where CIP version 6 is ordered before the CIP version 5 effective date (for medium and high, for example), but results in a CIP version 6 effective date after the CIP version 5 effective date. The implementation plan may not be supported until the low impact asset requirements are approved.
No comments.
Yes
Limit the applicability for dispersed generation to the point where those resources aggregate to greater than 75 MVA to a common point of interconnection at 100 kV or above and not at an individual turbine, inverter or unit level in the CIP-003-6 Applicability section similar to PRC-005. Suggested revision: Under the Introduction section, 4 Applicability, 4.2 Facilities, ***add the following statement after 4.2.2 All BES Facilities: “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back “for its assets identified in CIP-002-5.1 Requirement R1.3” in CIP-003-6 R2. The SAR for the CIP version 5 revisions project 2014-02 includes the following statement, “This project may also consider input that may be provided from CIP version 5 transition activities, for example from the NERC transition study or CIP Version 5 transition program.” At least one NERC transition study participant has identified the need to address dispersed generation in the CIP standards. Also, the dispersed generation project 2014-01 SAR includes the following phrase, “for standard drafting teams developing new or revised Standards, so that they do not incorrectly apply requirements to dispersed generation unless such an application is technically sound and promotes the reliable operation of the BES.” // Correct the errata in the Guidelines and Technical Basis for CIP-007-5 R2.2 in the last sentence of the second to last paragraph where it references a TFE. Technical feasibility exceptions are not included in Requirement R2.2 of CIP-007-5. // MidAmerican Energy Company supports Edison Electric Institute comments. MidAmerican Energy Company thanks the Standards Drafting Team for their technical competence, diligent work and collaboration with industry.
Individual

Michelle Clements
Wolverine Power Supply Cooperative, Inc.
Individual
Dan Gibson
Kansas City Power & Light
No
R2 – Usage of the term “external routable protocol paths” should be officially defined by NERC before being able to “judge the sufficiency” of the newly introduced controls. Assumptions a responsible entity could make surrounding this term could lead to violations. The Guidelines and Technical Basis section includes numerous references to “belief” and “intent,” along with descriptions of what entities “should” be doing. The need for such language indicates that the requirement language is not able to stand on its own and results in a need to be audited by the Guidelines and Technical Basis section. In turn, language not intended to be a required action by the entity could result in a perceived additional requirement by those trying to understand the requirement. While the intent of the “Note:” section under CIP-003-6 R2 is understood, there is no way to effectively audit for the successful and complete implementation of CIP-003-6 Table R2 – Low Impact Assets without obtaining an inventory of considered assets and of authorized users. Auditors are not able to reliably issue a judgment of the effectiveness of an internal control or of adherence to requirements without ensuring that samples are pulled from a complete population. Furthermore, entities are not able to perform the functions outlined within the R2 requirements without having lists of authorized users, both for access authentication and monitoring purposes. R2.3.2 – In part because the reference to “physical access point(s)” is not in relation to a defined Physical Security Perimeter, the requirement is actually more stringent than that of CIP-006-6 R1.4 and could require more evidence in support of compliance. An entity may need to prove an evaluation was performed resulting in the derivation of an inventory of all potential access points for all Low Impact BES Cyber Systems at Control Centers. Furthermore, diagrams may be needed to support that monitoring has been considered and defined for all applicable access points. While intended to be helpful in aggregating all Low Impact BES Cyber Systems requirements into a single section, the table has resulted in a web of functionally similar, yet separated requirements that could result in confusion. KCP&L recommends that, wherever possible, the items from CIP-003-6 Table R2 – Low Impact Assets be moved to the appropriate functional section and included as an additional applicable system where requirements are also similar. R2.4 – The requirements established under R2.4 are redundant to CIP-005-5 R1. In order to effectively audit the implementation of such controls, inventories and lists will be required just as they will be for CIP-005-5 R1. Guidelines and Technical Basis Section 2.4 – The two sentences beginning with “The electronic access controls should address…” go beyond the purview of the language of the requirement and serve to dictate what “should” be addressed. It is recommended that these sentences be stricken from the Guidelines and Technical Basis section.
No
CIP-006-6: The current order and applicability for CIP-006-6 is inconsistent and does not logically flow. At no point is a requirement for use of a defined PSP introduced, yet a number of the requirements pertain exclusively to the existence of a defined PSP. Physical Access Control Systems, as defined by the NERC Glossary of Terms, are also not stated as being required. Due to the current combined applicability and requirements, an entity could theoretically have a High Impact BES Cyber System that does not reside in a PSP and does not have a Physical Access Control System. This could result in applicability of only CIP-006-6 R1.3 and R1.10, and a lack of requirement for operational or procedural controls to restrict physical access. While the entity would still have to achieve two or more physical access controls, the requirements never state that a PACS is required for a High Impact BES Cyber System to achieve this or that a PSP is required for any system. KCP&L recommends that either CIP-006-6 R1.1 be updated to require the use of a Physical Access Control System for High Impact BES Cyber Systems or that a new sub-requirement is created to require High Impact BES Cyber Systems to have a Physical Access Control System with defined operational or procedural controls to restrict physical access. In addition, consideration should be given to rewording some monitoring, logging, and alerting requirements to include monitoring, logging, and alerting provisions for non-PSP, physically protected areas. CIP-007-6 The term “nonprogrammable communication components located inside both a PSP and an ESP” is a new source of confusion and may require definition as an official NERC Glossary term. CIP-005-5 requires only for “Cyber Assets”

to reside within an ESP. Unofficial guidance has already been communicated by various Regional Entities in support of excluding non-Cyber Asset, nonprogrammable “devices” from the required ESP. Therefore, it is difficult to identify where a “nonprogrammable communication component” that is also not a Cyber Asset would be located inside an ESP. Additionally, while CIP-006-6 defines certain protections that must be afforded to a Physical Security Perimeter, there is no requirement stating that a device must reside within a defined PSP. Therefore, entities are allowed to utilize other operational or procedural control measures for protecting High and Medium impact ESPs. Even if a “nonprogrammable communication component” is defined as part of an ESP, it is possible that the “nonprogrammable communication component” will not reside within a defined PSP. It should also be noted that the addition of such language will result in increased burden for entities by nature of a backdoor requirement for documentation of all considered “nonprogrammable communication components” that are not NERC-defined “Cyber Assets.” The current proposed language applicable only to “nonprogrammable communication components located inside both a PSP and an ESP,” along with other PSP-specific requirements, may serve to discourage entities from creating defined PSPs around BES Cyber Systems.
No
Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described in the comments submitted by the Edison Electric Institute. While we have previously stated that additional controls are necessary in this area for security and to ensure reliability, implementation of such controls will need to occur with a view toward practicality and sustainability.
No
KCP&L believes that the definition of Transient Cyber Asset should be clear to ensure no unintended consequences from interpretations by stakeholders involved where direct connections of devices are anticipated. Physical and electronic access control to BES Cyber Systems is a critical component of securing the overall system, and such devices should be protected from inappropriate Transient Cyber Asset connections. But the definition of such lacks clarity and thus will lack consistency in application. The language around the Transient Cyber Asset and Removable media is silent and unclear where EACMS and PACS are concerned. The new definition could read as follows: Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, or (2) a network within an ESP. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. Note: Clarity needed for issues identified previously.
Yes
While KCP&L supports alternative methods of assessing maturity and effectiveness in adherence to the NERC CIP requirements, the “Identify, Assess and Correct” language was an open-ended and unstructured framework that would cause confusion and lead to the expansion of the scope of NERC CIP based on auditor judgment. This concept would be addressed in tools and frameworks accomplished through the Reliability Assurance Initiative (RAI), however, consistency in auditor training and approach will be critical to the success of the RAI program.
Yes
No
We are not aware of additional jurisdictions that should be considered at this time.
Yes
KCP&L would like to endorse those comments made in this question by the Edison Electric Institute.
Individual
Kalem Long
The Empire District Electric Company
No
Parts 2.2 through 2.6 all require us to "implement one or more documented processes that..." However, the measures are about the documentation of operational controls, and nothing to prove implementation. There is an inconsistency between the requirement and what will be needed to show compliance to the requirement.

No
Though the intent is appreciated, CIP-006 Part 1.10 adds ambiguity with the verbiage "an equally effective logical protection." An entity may believe that they are compliant with full evidence, but this may not meet what auditor believes is "equally effective."
Yes
No
EDE agrees with EEI's comments: "There is a consistency issue. The definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to; however, the definition for Removable Media is not. It can be implied that the definition refers to connection to applicable systems, but it is not clear. It would also be clearer to switch the order of the Removable Media and Cyber Assets in the last sentence. {Suggested Revision} Change the definition of Removable Media to: “Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
Yes
Though Empire votes to approve the removal of IAC, we agree with SPP that "We do appreciate the clarity that removing the IAC language will provide. There is a concern that we are being asked to approve standards based on a program that is currently under development. By the time that a Responsible Entity will see how RAI is applied in audit situations, these standards, with the IAC language removed, will long have been voted upon."
Yes
No
No

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02
CIP Version 5 Revisions

Consideration of Comments
Initial Comment Period

September 3, 2014

RELIABILITY | ACCOUNTABILITY




Table of Contents

Consideration of Comments: Project 2014-02 CIP Version 5 Revisions

The Project 2014-02 Standard Drafting Team (SDT) thanks all commenters who submitted comments on the draft Critical Infrastructure Protection (CIP) Reliability Standards. These Reliability Standards were posted for a 45-day public comment period from June 2, 2014 through July 16, 2014. Stakeholders were asked to provide feedback on the Reliability Standards and associated documents through a special electronic comment form. There were 98 sets of comments, including comments from approximately 196 different people from approximately 142 companies representing all 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the CIP Version 5 Revisions SDT project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, please contact Valerie Agnew, the Director of Standards, at 404-446-2566 or valerie.agnew@nerc.net. There is also a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process can be found in the Standard Processes Manual.
http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Introduction

The SDT appreciates industry comments on the revisions to the CIP Reliability Standards. During the development of the revised standards prior to posting, the SDT made it a priority to conduct outreach as modifications were made to the standards. The SDT conducted two face-to-face meetings to revise the standards, Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs) in order to appropriately consider all comments received. The SDT continued its rigorous conference call schedule as it understands the importance of getting these standards to steady state.

Background

On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards and also directed that NERC make the following modifications to those standards:

1. Modify or remove the "identify, assess, and correct" (IAC) language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for to assets containing low impact BES Cyber Systems.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the IAC language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the low impact and transient electronic devices directives. The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.

Question 1: CIP-003-6

1. *The Standard Drafting Team (SDT) developed objective criteria in the processes in CIP-003, Requirement R2 to address the directive in FERC Order No. 791. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.*

Question 1 deals with the directive to develop modifications to the CIP standards to address security controls for assets containing low impact BES Cyber Systems. The SDT sought comments on its approach in modifying CIP-003-6, Requirement R2.

Placement

During the development prior to the initial posting, the SDT discussed the placement of the low impact requirements on many occasions. There were many commenters who suggested spreading out the requirement parts into the relating standards (for instance, CIP-008 for incident response), while a similar amount of commenters suggested keeping the requirements in CIP-003. The commenters supporting the allocation of the low impact requirements to the relating standards suggested to use existing applicability tables and sought justification for why the low impact requirements were in CIP-003 Requirement R2. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require a plan to address the Order No. 791 directive for more objective criteria. The applicability tables are no longer being used.

In response to comments that CIP-003 is a policy standard, the SDT developed the attachment approach where the requirement requires a plan whose elements are detailed in an attachment to the standard. The team also added language to CIP-003 clarifying that Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. The SDT discussed the costs and benefits of the placement issue and came to the conclusion that having the low impact requirements reside in CIP-003 was the best approach because it allows those with only assets containing low impact BES Cyber Systems to focus on one standard. As well, the SDT determined that an entity's management of low impact protections may differ from the medium and high impact protections (such as site level program implementation versus device level program implementation) and therefore the requirements are best suited to reside in one standard.

Reference to CIP-002-5.1

CenterPoint Energy questioned why the SDT deleted the link back to CIP-002-5.1, Requirement R1, Part 1.3. The SDT had removed the link in the previous version believing using "low impact assets" was sufficient. In response to this comment, the SDT has updated the requirement language to return the link to CIP-002-5, Requirement R1, Part 1.3. The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System." The SDT states that this creates the direct link between the CIP-003-6, R2 and CIP-002-5, R1, Part 1.3 language.

Part 2.1

Pacific Gas and Electric, Colorado Springs Utilities, Phillips 66, Consumers Energy Company, City of Tallahassee, and Salt River Project supported the proposed Requirement R2, Part 2.1 as written for reviewing and obtaining CIP Senior Manager approval.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, and Oncor suggested allowing a delegate for CIP Senior Manager approval of policies. In initial crafting of revisions based on industry comment, the SDT did provide the option for a delegate to approve the documented cyber security policies. However, in the most recent revisions,

the SDT rolled the low impact policy requirements into the existing Requirement R1. In that requirement, CIP Senior Managers and not delegates must sign off on the policies for any impact rating. Therefore, only the CIP Senior Manager can approve the policies applicable to assets containing low impact BES Cyber Systems under Requirement R1, Part 1.2.

For the applicability, Exelon proposed "BES Assets containing Low Impact BCS." In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System."

Dominion suggested removing the word "applicable" because it would have to apply controls at Control Centers even if it does not have one. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the evaluation of specific elements related to the assets containing low impact BES Cyber Systems. The evaluation provides the entity with the ability to determine applicability.

Part 2.2

ACES members asked if Part 2.2 was by site or collection of sites. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require a plan. Within the plan, the SDT has stated that entities can develop their plans by "asset or groups of assets."

Pacific Gas and Electric, Colorado Springs Utilities, Phillips 66, Consumers Energy Company, City of Tallahassee, TAL, and Salt River Project supported the proposed Requirement R2, Part 2.2 as written for restricting physical access.

Arkansas Electric Cooperative Corporation, PNM Resources Resources, Luminant Energy Company, LLC, and South Carolina Electric and Gas stated that restricting physical access does not provide sufficient criteria. The entities asked for clarification on what the difference is between operational or procedural controls. The entities also requested that the Guidelines and Technical basis section align with the requirement part language. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. Entities now evaluate possible physical security objective criteria and develop an entity-specific plan.

Similar to its comment for Part 2.1, Exelon proposed that the applicability read, "BES Assets containing Low Impact BCS." In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT is now using "The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System."

Part 2.3

Pacific Gas and Electric, Colorado Springs Utilities, Phillips 66, Consumers Energy Company, City of Tallahassee, TAL, and Salt River Project supported the proposed Requirement R2, Part 2.3 as written for monitoring.

Dominion and Xcel Energy commented to remove this requirement part completely since the breakout of Control Centers is contradictory to FERC Order No. 791. In response, the SDT agrees and has removed the reference to Control Centers.

Duke Energy pointed out that it is difficult to determine and monitor physical access points for lows. Duke suggested requiring a Physical Security Perimeter (PSP) to capture the intent. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. Registered Entities now evaluate possible physical security objective criteria and develop an entity specific plan.

Kansas City Power & Light commented that because reference to physical access points is not in relation to defined PSP, the requirement part is more stringent than CIP-006-5, Requirement R1, Part 1.4. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. Entities now evaluate possible physical security objective criteria and develop an entity-specific plan.

Similar to its comments for Parts 2.1 and 2.2, Exelon proposed that the applicability read, "BES Assets containing Low Impact BCS." Exelon further asked who is considered a visitor. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System." The SDT no longer has specific carve-outs for "Control Centers." With regard to the visitor question posed by Exelon, the SDT has removed that language from the requirement part and attachment, as well as the Guidelines and Technical basis section.

Part 2.4

Northeast Power Coordinating Council, Pacific Gas and Electric, Colorado Springs Utilities, Tennessee Valley Authority, Dominion, Edison Electric Institute, Florida Municipal Power Authority, NiSource, Oncor Electric Delivery Company LLC, PPL NERC Registered Entities (multiple), PacifiCorp, Western Area Power Administration, Large Public Power Council, Tacoma Public Utilities, New York Power Authority, Sacramento Municipal Utility District, Hydro One, Kansas City Power & Light, NV Energy, Salt River Project, Austin Energy, Northeast Utilities, Independent System Operator/Regional Transmission Organization (ISO/RTO) Standards Review Committee (ISO/RTO SRC), Luminant Energy Company, LLC, and South Carolina Electric and Gas had comments on the phrase "external routable protocol paths." There were concerns that this phrase implies some sort of Electronic Security Perimeter (ESP) and inventory, as well as suggestions to address "untrusted" networks (those not owned by the entity). Clarifications were requested to what the phrase means and, more specifically, what "external" was in reference to. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT does not use the phrase "external routable protocol paths" and has created definitions for Low Impact BES Cyber System Electronic Access Point (LEAP) and Low Impact External Routable Connectivity (LERC) to further clarify the lows requirement.

CenterPoint Energy, Bureau of Reclamation, and Duke Energy suggested consider of using "authentication" instead of "access control." In response, authentication was considered by the SDT, but the implications of a required list prevented this inclusion. The SDT states that the language as stated does not require a firewall to control access. The SDT developed two definitions and added explanatory guidance to help clarify the intent of the "access control" requirement.

PACIFIC GAS & ELECTRIC, Colorado Springs Utilities, Florida Municipal Power Agency, Xcel Energy, Idaho Power, Hydro One, and Exelon Companies stated that this requirement part implies an inventory must be done to prove compliance. In response, the SDT notes that an inventory may be the best option for proving compliance, but is not the only option and is not the required option.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Oncor Electric Delivery Company LLC, Associated Electric Cooperative, Inc., Phillips 66, Liberty Electric Power LLC, and Georgia Transmission Company commented that requiring justification for every firewall rule results in a significant amount of man-hours. Furthermore, the entities suggested to remove or reduce the part to not include inbound and outbound access permissions and remove the reason for granting access. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. The electronic access controls have been modified to "For any Low Impact External Routable Connectivity, establish a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all

other access." The SDT has removed "reasons for granting access." The SDT has modified the Guidance to explain that entities should maintain some documentation and be able to explain why the access permissions are in place.

Nebraska Public Power District and MidAmerican Energy Company suggested removing "default" as written as it appears that a firewall is the only solution. In response, the SDT removed "by default" and the language as stated does not require a firewall to control access. The SDT included additional discussion in the Guidance section for element 2.4.

Consumers Energy Company commented that the part should clearly state access points can reside either at the sub or at remote end of external routable protocol path. In response, the examples provided in guidance depict examples that the access points can be at the substation specifically or located at a regional or centralized location.

Massachusetts Municipal Wholesale Electric Company suggested to align this part more closely with CIP-005 because by avoiding the ESP and Electronic Access Point (EAP) requirements it becomes difficult to interpret and less effective at protecting. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. The SDT has created two new definitions for Low Impact BES Cyber System Electronic Access Point (LEAP) and Low Impact External Routable Connectivity (LERC).

Part 2.5

Northeast Power Coordinating Council commented that the incident response plan requirement part is inconsistent with CIP-008-5 Requirement R2's incident response plan for Medium/High. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Tennessee Valley Authority and Exelon asked if one incident response plan can encompass multiple facilities/BES Cyber Systems and if testing of the plan means that testing must occur for each facility. In response, the SDT has modified the approach to require that entities with assets containing low impact BES Cyber Systems develop a plan to address objective criteria in CIP-003-6, Attachment 1. The team intends for entities to have the latitude to develop a plan encompassing multiple facilities if they see fit and added "Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets" to the Attachment language. Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans.

Florida Municipal Power Authority, Tampa Electric Co., and Southern suggested limiting the scope of part 2.5 to low impact Control Centers and removing any reference that might include out-of-scope terms such as ESPs and PSPs. In response, the SDT has removed all specific carve-outs to "Control Centers."

Large Public Power Council commented that CIP-003 Requirement R2, Part 2.5 for low impact BES Cyber Systems should be added to the CIP-008 standard maintaining the 36 calendar months timeframe specific to low impact BES Cyber Systems. In response, the SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Phillips 66 commented that the incident response plan is duplicative of EOP-004 that covers cyber incidents. In response, the SDT states that the Cyber Security Incident response is required to be a part of the CIP standards and not covered in EOP-004.

Tampa Electric Co. and Southern suggested removing the word "paper" to allow for all types of drills. In response, the SDT has modified the incident response elements with the plan.

Consumers Energy commented that the language of the standard needs to clarify that the Responsible Entity can create a holistic incident response plan utilizing physical security mechanisms that lead to Cyber Security Incident identification, classification, and response; and that logging and monitoring of low impact BES Cyber Systems is not required. In response, the SDT has utilized language from CIP-008-5, which is exclusive to cyber security.

Lincoln Electric System recommended either removing Requirement R2, Part 2.5 or add an exclusion for 'Low Impact assets without routable connectivity' in recognition that a cyber-incident at a non-routable connected substation does not affect any other Low, Medium or High Impact BES Asset. In response, the SDT has utilized the language from CIP-008-5, which is exclusive to Cyber Security and does not exclude non-routable connections.

Idaho Power and PNM Resources suggested moving part 2.5 to CIP-008. Similar to the comments earlier regarding placement, the SDT notes that keeping the low impact obligations in one standard is the best place for the objective criteria to reside based on feedback from industry. The SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Exelon suggested the SDT provide clear guidance stating that sites with low impact BES Cyber Systems may be covered by an enterprise-wide Cyber Security Incident response plan or other approach, and assurance that a Cyber Security Incident response plan is not required for each site. In response, the SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Southern Company suggested providing additional information in the Guidelines and Technical Basis section on the use of the term "Cyber Security Incident" as it applies to low impact BES Cyber Systems. In response, the SDT has added language in the guidance that the entity should have a documented Cyber Security Incident response plan that includes each of the topics listed. For assets that have limited or no connectivity external to the asset, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a Cyber Security Incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Part 2.6

CenterPoint, Northeast Power Coordinating Council, Dominion, Edison Electric Institute, Large Public Power Council, Southern, NiSource, Public Service Enterprise Group, New York Power Authority, Xcel, PNM Resources, Exelon, NV, American Electric Power, Georgia Transmission Corporation, Northeast Utilities, MEC commented that the level of detail for security awareness is beyond what is required for mediums and highs. In response, the SDT has modified the language for security awareness to align with CIP-004, Requirement R1.

Tennessee Valley Authority, Idaho Power, PNM Resources, Exelon, and MidAmerican stated that this part should be located in CIP-004. In response, the SDT notes that keeping the low impact obligations in one standard is the best place for the objective criteria to reside based on feedback from industry. The SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Edison Electric Institute, Tampa Electric Co., NiSource, and Oncor suggested removing the references to the subpart requirements as they may not apply to all entities. The commenters also suggested removing the quarterly component. In response, the SDT has modified the language for security awareness to align with CIP-004.

PPL, Edison Electric Institute, Tampa Electric Co., Southern, Phillips66, NiSource, Public Service Enterprise Group, Xcel, and NV Energy recommended removing the language surrounding quarterly and modifying it to annually. In response, the SDT has modified the language to “at least once every 15 calendar months” from “quarterly.”

Consumers Energy commented that the language of the standard needs to clarify that the Responsibility Entity’s security awareness program applies only to its employees, but could include non-employees, and that posters, emails, and topics at staff meetings are sufficient delivery method and that tracking of reception is not required. LES had a similar comment regarding how security awareness is provided and proven on a per asset basis. In response, the SDT notes that methods of delivery are addressed in the guidance, and that the scope of awareness training is left to Responsible Entities to determine (non-employee vs. employee).

Dispersed Generation Resources (DGR)

Edison Electric Institute, Tampa Electric Co., NiSource, Oncor, We Energies, PNM Resources, Exelon, NV Energy, Florida Power & Light, and MidAmerican commented that the scope of dispersed generation in the CIP-003-6 Applicability section should be limited and similar to PRC-005. In response, the CIP SDT notes that coordination with the DGR SDT has been occurring and will continue to occur. Since CIP-002-5.1 is not being revised from the FERC Order No. 791 directives, the DGR SDT is best suited to modify the applicability and post the revised changes to CIP-002-5.1 for an initial comment and ballot period. Not slated as a “high priority standard” in the DGR’s project plan, CIP applicability changes can fall into the DGR’s “medium priority” bucket as it continues its work on modifying certain standards to address dispersed power producing resources. The DGR SDT has an upcoming meeting in September 2014 and the CIP applicability change is on its agenda. The CIP SDT will continue to coordinate with the DGR SDT as necessary to provide technical basis and justification for any work the DGR SDT provides in revising CIP-002-5.1. A timeline for that posting should come out relatively soon to give commenters assurance that work will continue through the DGR SDT’s SAR.

Reliability Standard Audit Worksheets (RSAWs)

Pacific Gas & Electric recommended the performance of an annual sampling assessment of such classified systems to determine the state of their security controls. This could be done using NERC sampling guidelines. In response, the SDT notes that this is most appropriately addressed through the RSAW approach.

Florida Municipal Power Authority commented that the RSAWs do not provide any level of clarity as to how an entity can expect to be audited. Large Public Power Council, Tacoma, New York Power Authority, and Sacramento Municipal Utilities District commented that specific RSAWs can be created for the low impact requirements that reduce the number of RSAWs that need to be completed by entities. In response, the SDT notes that there is a

specific RSAW working group focused on revising the posted RSAWs. That team will take into account the RSAW comments and revise them accordingly.

Exelon encouraged the RSAW development team to continue its work in modifying the RSAWs and possibly include RAI components for the assets containing low impact BES Cyber Systems to demonstrate how RAI can alleviate compliance concerns. In response, the SDT notes the RSAW working group will take into account the RSAW comments and revise them accordingly.

FirstEnergy had concerns with the RSAWs and support Edison Electric Institute's comments. In response, the SDT notes that there is a specific RSAW working group focused on revising the posted RSAWs. That team will take into account the RSAW comments and revise them accordingly.

General Comments

CenterPoint commented that Measure M2 should be revised to reflect the pattern in other Measures of CIP-003. CenterPoint further suggested that the SDT consider the pattern found in other standards and remove the word "any" from the draft Measure. In response, the SDT has made the appropriate modifications to the Measures based on the revised language in CIP-003.

Edison Electric Institute, Tampa Electric Co., NiSource, Oncor, and We Energies suggested revisions to the background and guidelines and technical basis sections to align the drawings and the words of the requirement. In response, the SDT has modified the current language to remove the table within Requirement R2, electing to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Duke Energy commented that there are the same control measures in place as medium impact BES Cyber Assets, which will become extremely burdensome and provide little benefit to reliability. In response, the SDT has modified the language to ensure a compliance burden less than high and medium impact BES assets based on risk to the BES.

Southern commented that the Applicable Systems column should be amended to state "Assets containing low impact BES Cyber Systems." In response, the SDT has modified the current language to remove the table within R2, electing to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Rayburn asked if the standard sufficiently covers the appropriate levels and tactics expected to be used to be compliant. In response, the SDT has modified the current language to remove the table within R2, electing to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Dynegy requested the SDT provide guidance in the standard as to how to determine low impact BES Cyber Systems without using the detailed inventory process. In response, the SDT has modified the current language to maintain "policy and program" level within the requirement and include additional objective language within an associated Attachment.

Occidental commented that subjective interpretations by Regional Entities are still a very real concern. In response, the SDT has forwarded the comments to NERC.

Idaho Power suggested that the applicability section of all these requirement parts addresses low impact BES Cyber Systems. It is counterintuitive to think that a list of low impact BES Cyber System will not be required to show compliance. In response, the SDT states that anticipating high counts of low impact BES Cyber Systems, the

SDT intends to allow Responsible Entities to shift their compliance approach away from rigorous Cyber Asset list maintenance and toward consistent maintenance of the low impact controls identified in CIP-003-6. The SDT believes the list of assets containing low impact BES Cyber Systems generated as a result of CIP-002-5.1, R1 is sufficient. However, Responsible Entities are not prohibited from developing and maintaining individual inventories of their low impact BES Cyber Systems components for their own business needs.

Hydro One suggested modifications to the VSLs. The SDT has made the revisions to the VSLs.

Encari commented that the Guidelines and Technical Basis section continues to use "external routable connectivity" in the discussion of Requirement R2 in parts 2.3 and 2.4. In response, the SDT has modified the current language to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Kansas City Power & Light suggested that the Guidelines and Technical Basis section includes references to "belief" and "intent" along with descriptions of what entities "should" be doing. The need for such language indicates that the requirement language is not able to stand on its own and results in a need to be audited by the Guidelines and Technical Basis section. Section 2.4 - The two sentences beginning with "The electronic access controls should address..." go beyond the purview of the language of the requirement and serve to dictate what "should" be addressed. It is recommended that these sentences be stricken from the Guidelines and Technical Basis section. In response, the SDT has modified the Guidelines and Technical Basis section throughout the standard based on the comments received and the revisions made.

Nebraska Public Power District commented that while the drafting team has tried to show in the guidance what would be acceptable and what would not, in essence they have determined the "how" the requirement will be audited by showing only a firewall solution. In response, the SDT has modified the language to provide clearer objective criteria which allows for flexibility to Registered Entities.

American Public Power Association and National Rural Electric Cooperative Association commented that the SDT has gone too far in certain aspects of specificity of the requirement parts and the compliance costs exceed the reliability benefit to the BES. In response, the SDT has modified the language to provide clearer objective criteria and allows flexibility to Registered Entities. This allows for entities to tailor their internal plans to cover the risk that to assets containing low impact BES Cyber Systems pose.

National Rural Electric Cooperative Association recommended that NERC use the Requirements on low impact assets to demonstrate how RAI can alleviate the compliance concerns and create a reasonable approach to compliance. The SDT notes that it has forwarded these comments on to NERC.

Northeast Utilities commented that there are inconsistent testing time frames. Instances where there was a failure to extend implementation time-frame beyond the original version 5 effective compliance date. In response, the SDT has modified the implementation schedule to address inconsistencies.

MidAmerican provided suggested revisions to the Background section to include a paragraph referencing the tables and applicable systems column. The SDT has modified the approach to the low impact directive. The tables and applicable systems column are no longer being used.

Empire commented that the measures are about the documentation of operational controls and show nothing to prove implementation. There is an inconsistency between the requirement and what will be needed to show compliance to the requirement. In response, the Measures have been revised according to the revisions made to the Requirement and Attachment 1. A Measure provides identification of the evidence or types of evidence that

may demonstrate compliance with the associated requirement. Entities must show evidence of implementation of their plans to demonstrate compliance to the Requirement.

Southwest Power Pool Regional Entity disagreed with the premise in the Guidelines and Technical Basis section of the standard that compliance can be demonstrated purely through presentation of the documented processes at audit. There is an expectation that the documented processes will be implemented by the Responsible Entity. The guidelines should inform the Responsible Entity and the auditor what is expected to comply with the requirements and not how the requirements should be audited. The comment that the SDT strongly believes sampling is not necessary is inappropriate and should be removed. In response, the SDT has revised this section and removed the sampling component from this section.

Manitoba Hydro commented that section C of the Compliance section 1.3 is unclear, specifically that the meaning of “Complaints Text” is unclear. In response, the SDT has removed the word “Text” to be consistent with the other NERC Reliability Standards.

Luminant provided suggested revisions to multiple aspects of the Guidelines and Technical Basis section. The SDT has considered those suggestions as it went through the section as a whole and provided updates based not only on comments received, but also on the revisions made to CIP-003-6.

Massachusetts Municipal Wholesale Electric Company suggested that the Implementation Plan allow for a phased in approach. In response, the SDT agrees and has proposed a phased approach to the Implementation Plan allowing an additional implementation time for physical and electronic access.

Question 2: CIP-006-6 and CIP-007-6

2. *The SDT developed CIP-006, Requirement R1, Part 1.10 and revised CIP-007, Requirement R1, Part 1.2 to meet the directive in FERC Order No. 791 to address protections for nonprogrammable components of communication networks. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.*

Question 2 deals with the directive to create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

CIP-006-6, Requirement R1, Part 1.10

Encryption

In response to ISO/RTO SRC and Tennessee Valley Authority, the SDT does not believe the Reliability Standards are an appropriate location for approved cryptographic protocols. This is due primarily to the ever-changing number of protocols and vulnerabilities in cryptosystems. Also, an approved encryption concerns both protocol and implementation. This type of information is best left to guidelines.

ERCOT suggested a Critical Infrastructure Protection Committee (CIPC) guideline be developed on acceptable encryption protocols, methods, and key management. In response, the SDT notes that CIPC may develop guidelines as part of its charter, which states that guidelines are documents that suggest approaches or behavior in a given technical area for the purpose of improving reliability. Reliability guidelines are not binding norms or mandatory requirements. Reliability guidelines may be adopted by a Responsible Entity in accordance with its own facts and circumstances. Any entity may submit a request for the CIPC to develop guidance, and the SDT will consider this suggestion after the second posting and discuss with NERC staff.

American Public Power Association and Florida Municipal Power Authority showed support for encryption as an option, but would reevaluate if encryption were removed or scope expanded. The SDT thanks those entities for their comments.

Tampa Electric Co. commented that monitoring the status of communication link is duplicative of COM-001-1.1 R1.1. Failure of communication links does not necessarily need to be reported through the BES Cyber Security Incident Response Plan. In response, the SDT states the communication link failure is specific only to the nonprogrammable components outside of the PSP and not the communication to other entities covered by COM-001-1.1 R1.1. The incident response component is only necessary if the monitoring/response option is used to protect the cabling and components. The incident response is included because monitoring alone does not provide the necessary physical security to the BES Cyber System.

NextEra Energy commented that rather than allow encryption and monitoring, require secure conduit, cable trays or defense-in depth approach for the BES facility. In response, the SDT notes that secure conduit and cable trays meet the obligation to restrict physical access. These options are mentioned specifically in the Guidelines and Technical Basis section for CIP-006-6. The defense-in-depth approach for the BES facility may also meet the same obligation, but encryption and monitoring are provided as specific and measurable options.

Tri-State commented that for monitoring controls, a 15-minute window for notification is typically not enough time to respond to an event. In response, the 15-minute window is to issue the alert or alarm in response to an event. The actual response does not have a time obligation. The SDT agrees time measured responses are not appropriate for this requirement part.

Pacific Gas & Electric and Southwest Power Pool Regional Entity commented that for monitoring controls, a timeframe does not exist for response or investigation and that ignoring a momentary interruption could result in not detecting a tap. Also, for short-run cables, investigation is not feasible. In response, the SDT does not believe a time obligation for response is appropriate for this requirement part. Operational variances in responding to an incident are best left to the entity's incident response plan. In response to Southwest Power Pool Regional Entity regarding tap detection, the entity would contemplate this scenario when selecting this option for protection. The SDT states that the controls, as written, sufficiently guard against this risk.

Pacific Gas & Electric recommended that for monitoring controls, a CIP Senior Manager sign-off should be required to ensure implementation remains intact as designed. In response, the CIP Senior Manager sign-off would not change the obligation for the entity. An entity may choose to employ a sign-off as part of their internal controls program, but this should not be a requirement.

Kansas City Power & Light commented that a Physical Access Control System (PACS) or PSP is not specifically required, and it may be possible to comply with CIP-006 without having a PACS or PSP. Kansas City Power & Light suggested requiring these as part of CIP-006 Requirement R1. In response, this comment is outside the scope of the Standards Authorization Request for this project. A PSP is not specifically required because an entity may be able to meet the objectives of physically securing the BES Cyber System without a PSP or PACS.

Tacoma Public Utilities stated a concern that a detailed cable map for every cable path relevant to the ESP will be required to demonstrate compliance. In response, the obligation to maintain a detailed cable map is not a Requirement of the Reliability Standards. The SDT has passed these concerns to the NERC Compliance staff to guide development of the RSAW.

Exelon suggested clarification that applicability only applies to ESPs with External Routable Connectivity. The SDT has provided additional guidance to clarify the bounds of this Requirement Part is the ESP. By definition, Electronic Access Points provide External Routable Connectivity.

Luminant Energy Company commented that for CIP-006-6 R1 and R2, a reason for removing all but the Severe VSL needs to be provided. For example, what if an entity had a process to retain logs for 90 days but instead retained all of the logs? In response, the CIP-006 VSLs have been binary (i.e. Severe only) since version 2 because of the FERC Order addressing VSLs for CIP stating: "Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary rather than gradated Violation Severity Levels."

Equally Effective Solution and Suggested Revisions

Dominion, Bureau of Reclamation, Xcel Energy, Texas Reliability Entity, Tri-State, Empire District, Southwest Power Pool Regional Transmission Organization, ISO/RTO SRC, ERCOT asked how "equally effective logical protection" be measured. The commenters suggested possibilities: (1) equal to other options, (2) describe how protection would be measured, (3) cable travels through facilities that provide physical access only to authorized personnel, (4) use of armored wire, (5) level of encryption, or (6) altogether removal of the 3rd bullet. In response, the SDT notes that the intent of including other effective logical protection is to allow entities the option of defining this protection. An entity may demonstrate compliance by showing how it protects the cabling and nonprogrammable components similar to the other options listed in the Requirement Part. The guidance for CIP-006-6 has been updated to make this clear. The specific suggestion to have cable travel through facilities that provide physical access to only authorized personnel would be considered physical access restrictions and has been included in the Guidelines and Technical Basis of CIP-006-6. The use of armored wire is functionally equivalent to the required physical access restrictions.

Similar to the comment raised above, Southwest Power Pool Regional Transmission Organization, ISO/RTO SRC, and Southern California Edison Company stated concerns on whether evidence will be necessary to show that physical access restrictions cannot be implemented. Suggestion to make clear that there is a choice between physical access restriction and alternative means of protection. In response, if an entity selects one of the alternatives in this Requirement Part, the Requirement language makes clear this is when such physical access restrictions *"are not"* implemented. Therefore, there is no additional obligation for the entity to demonstrate it cannot apply physical access restrictions. The Requirement leads with physical access restrictions to make sure the physical security objective is maintained.

Bonneville Power Administration and Massachusetts Municipal Wholesale Electric Company commented that control coverage is insufficient to provide adequate protection of the BES. Massachusetts Municipal Wholesale Electric Company further suggested CIP-006-6 should also include requirements for low impact BES Cyber Systems. In response, the SDT proposes the standards revisions as adequate and appropriate to protect the reliability of the BES. In doing so, the level of effort to meet the Requirement has been weighed against the risk posed to the BES.

CIP-007-6, Requirement R1, Part 1.2

Associated Electric Cooperative, Inc., National Rural Electric Cooperative Association, and American Electric Power stated that this requirement part is duplicative and overlaps with CIP-010-2 Requirement R4. In response, the Requirement to protect ports for Removable Media is different than the CIP-010-2 R4 Requirement for Removable Media. CIP-010-2 Requirement R4 concerns the Removable Media while CIP-007-6 Requirement Part 1.2 concerns the BES Cyber System ports.

Northeast Power Coordinating Council, New York Power Authority, and Hydro One suggested adding rationale for part 1.2 to the guidelines. Furthermore, the commenters suggested adding illustrative examples to the Measures and guidelines so entities and auditors will have the same interpretation. In response, additional clarification regarding the applicability has been added to the Technical Guidelines to make clear the scope of this Requirement Part as well as approaches to meeting the Requirement.

Duke and Exelon sought clarification that applicability means (a) devices located inside both a PSP and an ESP and not (b) devices within a PSP and devices within an ESP. Furthermore, the comments suggested the following for clarity: "Nonprogrammable communication components used for the connection between applicable Cyber Assets within the same ESP and within a PSP." In response, the SDT confirms that the applicability means devices located inside both a PSP and ESP. The SDT has added illustrations to the Guidelines and Technical Basis section to assist entities in understanding the applicability.

Associated Electric Cooperative, Inc. and National Rural Electric Cooperative Association sought more clarity around the term "nonprogrammable communication components." In response the SDT has provided additional examples in the Guidelines and Technical Basis that nonprogrammable communication components include unmanaged switches, hubs, and patch panels. This requirement only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and nonprogrammable communications components exist inside the PSP, that protection is afforded to these communication elements and therefore this requirement no longer applies. The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order No. 791 is one of the physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify

or explain why it chose another protection mechanism. It may choose physical security protections or the logical protections identified in the requirement at its choice.

Northeast Utilities requested additional guidance on meeting this requirement for patch panels. The entity asked, 1) if cyber assets in the ESP have disabled unnecessary ports and services, is additional protection necessary? And 2) is signage or tamper tape required for all ports that are not used or disabled? In response, there are several options to protect against the use of these unnecessary ports. The entity should select the controls that make the most sense in their environment. Disabling ports, signage or tamper tape are all possible controls.

Definitions

Consumers Energy Company, Kansas City Power & Light, and Exelon suggested defining "nonprogrammable electronic components." The SDT does not agree defining nonprogrammable communication devices would provide additional clarity. The SDT suggests the term with the use of examples provides the common understanding necessary to meet the new Requirements.

Idaho Power and Tri-State stated that this does not address the FERC directive to create a definition of communication networks and developing new or modified standards. In response, the SDT reviewed the directives related to submitting a definition for communication networks and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The existing and modified requirements cover more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.

Kansas City Power & Light raised a concern that entities will have an obligation to keep an inventory of nonprogrammable electronic components. In response, the obligation to maintain an inventory of nonprogrammable electronic components is not a Requirement of the NERC Reliability Standards. The SDT has passed these concerns to the NERC Compliance staff to guide development of the RSAWs.

Question 3: CIP-010-2

3. *The SDT developed CIP-010, Requirement R4 and revised CIP-004, Requirement R1, Part 2.1.9 to meet the directive in FERC Order No. 791 to address transient devices (Transient Cyber Assets and Removable Media). Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.*

Applicability and Placement

ISO/RTO SRC, FirstEnergy, and Tacoma Public Utilities commented to move the requirement parts to the applicability of relevant CIP-007 requirements. In response, the SDT has not moved the requirements to the applicability of other standards. Since the use of these devices is limited to the context of change management and vulnerability assessment, the SDT determined that placing the requirements within CIP-010 is appropriate. While the requirements are similar to other standards, the requirements for Transient Cyber Assets and Removable Media are not the same as the requirements for BES Cyber Systems and other permanent assets.

Encari suggested that the applicable systems should be expanded to include the EACMS and PACS that are associated with high and medium impact BES Cyber Systems. In response, the SDT has chosen to focus the requirements to the assets that are to be connected to the BES Cyber Systems that provide a BES reliability operating services, as well as those residing within the same ESP. The goal is to protect the systems that can have a direct impact on real-time operations.

San Diego Gas & Electric sought clarification that devices not directly connected to the BES Cyber System should be exempt or considered out of scope such that other devices or media that are connected to the Transient Cyber Asset would be out of NERC CIP scope. In response, the SDT considers any other Cyber Asset or Removable Media connected to a Transient Cyber Asset to require the same protections as the Transient Cyber Asset or any other Removable Media.

Duke Energy, Southern Company: Southern Company Services, Inc., Alabama Power Company, Southern Company Generation, Southern Company Generation and Energy Marketing, Luminant Energy Company, LLC, Exelon Companies, and MidAmerican Energy Company stated that there were inconsistencies in the use of the applicability part of the table. In response, the SDT notes the tables supporting CIP-010-2 Requirement R4 have been eliminated. Please refer to the definitions of Transient Cyber Asset and Removable Media for specifics of the assets in scope.

Measures

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Exelon Companies, Texas Reliability Entity, and Bureau of Reclamation commented that the measures do not align with the requirement language and that some of the measure language is unclear on the meaning. In response, the tables supporting CIP-010-2 R4 have been eliminated. The requirement obligates the entity to create and implement plans for Transient Cyber Assets and Removable Media. The measure supports this requirement. Clarification of many topics has been added to the guidance.

Guidance

CenterPoint Energy recommended removing examples of statements from Guidelines and Technical Basis to reduce redundancies with definitions of Transient Cyber Asset and Removable Media. The SDT notes that while the examples are similar to those in the definitions, the examples in the guidance are more defined and provide guidance that has been requested by industry.

Dominion requested additional language to clarify the phrase "per Cyber Asset capability." The SDT has modified the guidance to clarify "per Cyber Asset capability."

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing recommended striking the term "physical proximity" as this is not required by the standard as written. In addition, these entities recommended removing the phrase "process is to include testing and installing of updated signatures or patterns." In response, the SDT removed the language.

Edison Electric Institute and NiSource suggested the SDT correct inconsistencies in the "Applicable Systems" of the Guidelines and Technical Basis. The SDT modified the guidance to align to the attachment sections.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, and Luminant Energy Company, LLC suggested the SDT consider removing the bullets under "Examples of these devices include…" and consider strengthening the intended meaning of the list of examples to improve clarity and provide guidance to industry. The SDT considers the example list of asset types to be appropriate guidance for the industry. These are examples and are not intended to be an all-inclusive or exhaustive list.

Edison Electric Institute, NiSource, San Diego Gas & Electric, and MidAmerican Energy Company commented that the guidance goes beyond the scope of the standard in Bullet 2 under Requirement Part 4.1 of the guidance because it includes low impact. These entities further commented that the SDT should consider that transient devices should be required to have a uniform level of protection sufficient to ensure that a designated and approved transient device could be used at any facility. The SDT notes that the requirements do not apply to low impact. However, the SDT believes it is worth providing guidance to the industry that the higher impact assets should be protected from the vulnerabilities from any other asset.

Southwest Power Pool Regional Entity and Northeast Utilities recommended that the SDT add alternatives to the use of anti-malware in the Guidelines and Technical Basis. The SDT modified the standard to include an attachment with options that may be applied to address malware prevention.

Tampa Electric Company recommended clarification of the Guidelines to allow for Removable Media to be validated on a periodic basis instead of on a per-use basis. The SDT modified the requirement to obligate the entity to create and implement management plans for Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization.

Northeast Utilities suggested the SDT expound upon the "CAUTION" statement in the Guidelines and Technical Basis regarding the use of secure wireless network to only access a secured network drive containing relay configuration data. The SDT defined more guidance and Requirement language for the use of secure, restricted communications in Attachment 1.

Part 4.1 – Authorization

Dominion, Duke Energy, Large Public Power Council, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Florida Municipal Power Authority, Exelon Companies, Austin Energy, and National Rural Electric Cooperative Association commented that the requirement to authorize "Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability)" should be removed. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that

are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, and American Electric Power requested Requirement R4, Parts 4.1 and R4.6 be applicable to just high impact BES Cyber Systems and their associated PCAs and Part 4.1 be removed or modified to apply to medium impact BES Cyber Systems with External Routable Connectivity. In response, due to the wide-area impact of the high and medium impact assets, the SDT considers the application of these requirements to these assets as appropriate. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization.

Hydro One commented that the requirement Part 4.1 should state clearly who can authorize the Transient Cyber Assets. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. Any process or plan meeting compliance requirements should be owned and maintained by the appropriate parties within the entity's organization.

ISO/RTO SRC, MidAmerican Energy Company, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing commented that: 1) Authorization should include purpose for connecting the Transient Cyber Asset, start date/time, duration, and which ESPs the Transient Cyber Asset is authorized to connect to; 2) Authorization of acceptable use exceeds FERC's directive; and 3) Acceptable use should not be required to be "authorized" for each initial use of a Transient Cyber Asset, but should be separated to allow for addressing acceptable use at the policy/procedure level. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions. This also allows for assets to be documented individually, by group, or by type.

Hydro One, ISO/RTO SRC, MidAmerican Energy Company, Oncor Electric Delivery Company LLC, PACIFIC GAS & ELECTRIC, Salt River Project, and South Carolina Electric and Gas recommended revising or removing the phrase "internally installed software," requested revision of the language to allow for pre-authorized operating system, firmware, and intentionally installed software, and recommended changes to require sampling of transient devices security baselines. In response, The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions. This also allows for assets to be documented individually, by group, or by type.

MidAmerican Energy Company, Edison Electric Institute, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, NiSource, and NV Energy commented that authorization of users should not be required for the Transient Cyber Asset if users are already authorized for the applicable systems. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. In response, the SDT modified the requirement to obligate the entity to create

and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard. The entity could use its other authorization processes to document those authorized to use Transient Cyber Assets in its plan. However, the entity needs to review the appropriateness for every person with physical access to a facility or every user with logical access to a BES Cyber System to be able to use a Transient Cyber Asset.

South Carolina Electric and Gas, Dominion, and Pacific Gas & Electric 1) recommended language changes to allow entities to implement controls and maintain flexibility to address multiple device types and functions; 2) Requested clarification that allows entities to authorize classes or groups of Transient Cyber Assets; and 3) Requested revisions to require procedures defining the acceptable use of Transient Cyber Assets and a listing of authorized Transient Cyber Assets. Such a list needs to be generic allowing entities to authorize groups of Transient Cyber Assets. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. The plan allows for assets to be documented individually, by group, or by type.

Parts 4.2, 4.3, 4.4, and 4.5 - Malware

City of Tallahassee, ISO/RTO SRC, and Hydro One stated that parts 4.2 and 4.3 appear to be identical. In response, while the requirements are similar, there are key differences. Cyber Assets are programmable devices that may be capable of running antivirus. Removable Media are not programmable, and therefore unable to run antivirus.

Southwest Power Pool Regional Entity suggested that CIP-010-2, Part 4.2 could be construed as mandating anti-malware on a transient device. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including optional provisions for mitigation of vulnerabilities.

Tampa Electric Co. suggested that the SDT should add the “per device capability” to CIP-010-2 R4 Part 4.3 to address device limitations. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard including provisions for mitigation of vulnerabilities. “Per Transient Cyber Asset capability” is addressed where appropriate within the attachment.

American Electric Power, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Exelon Companies, ISO/RTO SRC, and Hydro One requested clarification that remediation or updating completion is required prior to use of the device and clarification on the handling of discovery of malicious code following connection of the device to a BES Cyber System. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including optional provisions for mitigation of vulnerabilities. Elements were added to the attachment that require the device to be managed or updated on demand before connection to an applicable BES Cyber System.

National Rural Electric Cooperative Association commented that Part 4.4 focused on mitigating the threat of malicious code to Transient Cyber Assets and Removable Media but should focus on protecting the BES Cyber Asset. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the

program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard including provisions for mitigation of vulnerabilities. “Per Transient Cyber Asset capability” is addressed where appropriate within the attachment.

Part 4.6 - Inspection

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Florida Municipal Power Agency, and Duke Energy commented to consider requiring the definition of acceptable use of Transient Cyber Assets, and the process to authorize usage and evaluation of Transient Cyber Assets. The commenters requested removal of CIP-010-2 Requirement R4, Part 4.1.4 and Part 4.6. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions.

Salt River Project recommended changing the language to address Entity-owned and -maintained transient devices separately from vendor or contracted support-owned and -maintained transient devices. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard including provisions for mitigation of vulnerabilities. The attachment addresses assets owned by the entity, as well as those owned by vendors and contractors.

Luminant Energy Company, LLC and ISO/RTO SRC suggested considering adding an additional requirement to remediate anything found in the evaluations conducted in accordance with the requirement related to patching or unauthorized physical access and requested strengthening of the requirement to mandate that remediation or updating completion prior to use of the device. In response, The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. The attachment requires implementation of one or more of the protective measures before connecting the device.

Dominion commented that clarity is needed regarding whether an entity expected to reauthorize the baseline list of “Operating system(s) or firmware where no independent operating system exists, and intentionally installed software” for a Transient Cyber Asset when it’s changed as a result of executing Part 4.6. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. This removed the concept of base-lines from the requirements.

Exelon Companies and Hydro One suggested to consider incorporating R4.6 into R4.1 and requested rewording of Requirement R4, Part 4.6. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities.

Part 4.7 - Patching

Southwest Power Pool Regional Entity, Tennessee Valley Authority, Edison Electric Institute, NiSource, Large Public Power Council, American Electric Power, MidAmerican Energy Company stated that CIP-010-2, Part 4.7 should require the transient device to be fully patched and not permit an alternative mitigation plan. The commenters suggested that clarification is needed that any mitigation of a vulnerability must be completed prior to use of the asset. Lastly, the commenters suggested that the requirement should clearly note that mitigation of a vulnerability is permitted in lieu of applying a patch, when justified. In response, the SDT states that there may be instances where patching the device is not permitted or advised. Therefore, the option to create a plan to mitigate the specific vulnerability addressed by the patch would be appropriate. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities.

Tampa Electric Co., Florida Municipal Power Authority, Large Public Power Council, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Exelon Companies, and ISO/RTO SRC sought clarification as to whether the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use. The commenters also had concerns with the need to track both the 35-day update timeframe and each use to be able to show performance to the requirement part, that the 35-day update requirement is more aggressive than for CIP-007, R2.2 and R2.3 that allow 35 days to evaluate and 35 days to install, and whether a single evaluation within 35 days prior to use would be sufficient to comply with the requirement. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. The attachment addresses assets owned by the entity, as well as those owned by vendors and contractors. The attachment also allows for the entity to perform activities either in a managed program state or through on demand activities.

Other

CenterPoint Energy, Kansas City Power & Light, and Southern California Edison Company commented that the administrative burden associated with Transient Cyber Assets and Removable Media is exceptionally challenging or even unattainable, and is not aligned with the risk introduced to the BES. In response, the tables supporting CIP-010-2 Requirement R4, have been removed since the initial posting. The requirement obligates the entity to create and implement plans for Transient Cyber Assets and Removable Media. The measure supports this requirement. Clarification of many topics has been added to the guidance.

Pacific Gas & Electric recommended language changes to require a security policy for transient devices. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan elements are addressed in Attachment 1 of the standard.

Bonneville Power Administration and Pacific Gas & Electric commented that the use of direct remote access should be prohibited and to consider an implementation of a method which allows vendors to perform their work without directly accessing systems. In response, the SDT states that any vendor connecting to a BES Cyber System remotely is subject to Interactive Remote Access requirements. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization.

Bonneville Power Administration suggested that the proposed requirement language should also address assets containing low impact BES Cyber Systems. In response, due to the wide-area impact of the high and medium impact assets, the SDT limited the requirements to these assets. This includes protection from lower impact assets.

Exelon Companies commented that the sentence in the rationale referencing the relative rigor should be removed. In response, the SDT notes that the sentence has been removed.

Southwest Power Pool Regional Transmission Organization, Hydro One, and Tri-State G&T, for CIP-004 Requirement R2, Part 2.1.9, suggested deleting the word "including" as neither TCAs nor Removable Media are Cyber Assets and also suggested removing the word "with." In response, the SDT notes Transient Cyber Assets are Cyber Assets. The requirement is to address the interconnection of Cyber Assets, which includes Transient Cyber Assets. The requirement is also to address the interconnection with Removable Media, which is not a Cyber Asset.

Bonneville Power Administration, Network & Security Technologies, MidAmerican Energy Company, Exelon Companies, and Luminant Energy Company, LLC commented that 1) the requirements should focus on transient devices at the time of connection; 2) the meaning of "use" and "prior to use" is ambiguous; and 3) there are concerns with having to track each and every use of the transient device. In response, the SDT notes that the requirement for Transient Cyber Assets and Removable Media is included in CIP-010 to allow entities to align their recordkeeping of the devices to the change management activities being supported. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard and are focused on addressing security vulnerabilities and malicious code protections.

Question 4: Definitions

4. *The SDT proposed new definitions for Transient Cyber Assets and Removable Media and revised definitions for BES Cyber Asset and Protected Cyber Assets. Do you agree with the new and revised definition? If not, please offer suggested revisions.*

BES Cyber Asset

Edison Electric Institute, NiSource, We Energies, PNM Resources Resources, and Oncor commented that the BES Cyber Asset definition is inaccurately quoted in the Guidelines and Technical basis in CIP-002-5.1. The SDT appreciates the comments but is not revising CIP-002-5.1 at this time. The scope of the SDT's Standard Authorization Request is focused mainly on the directives contained in FERC Order No. 791. Therefore, the SDT revised only those standards that should include language addressing the directives.

Nevada Energy suggested the SDT revise the guidance regarding BES Cyber Asset because it seems that devices whose loss could preclude a BES Reliability Operating Services (BROS) would be a BES Cyber Asset. The SDT appreciates the comments. The proposal to revise CIP-002-5.1 guidance is out of the defined Standards Authorization Request for this SDT, but we submit additional context in which the BES Cyber Asset and guidance language was drafted in CIP-002-5.1. The BES reliability operating services are provided in guidance to assist entities with a more granular description of adverse impact to the BES. For CIP Version 5, the more generic definition and specific guidance struck a balance with industry comments to provide enough granularity but still allow flexibility in the Requirement language.

Dominion and ISO/RTO SRC suggested moving the clarification on Transient Cyber Assets into that definition rather than keeping it in the BES Cyber Asset definition. The SDT removed the last sentence regarding Transient Cyber Assets from the BES Cyber Asset definition.

Protected Cyber Asset

Dominion and ISO/RTO SRC suggested moving the clarification on Transient Cyber Assets into that definition rather than keeping it in the Protected Cyber Asset definition. The SDT removed the last sentence regarding Transient Cyber Assets from the Protected Cyber Asset definition.

Transient Cyber Asset

Tennessee Valley Authority requested clarification on what "directly connected" means and if it includes specific media types. The SDT clarifies that "directly connected" means that there is nothing in between the Transient Cyber Asset and the Cyber Asset or network to which it is connected.

Southwest Power Pool Regional Entity commented that the Transient Cyber Asset definition is broad so that entities could disconnect assets categorized as BES Cyber Assets and Protected Cyber Assets as Transient Cyber Assets. ISO/RTO SRC questioned what would happen to a Transient Cyber Asset that has been connected longer than 30 days. The SDT considers any device connected for more than 30 days to be part of the BES Cyber System.

Kansas City Power & Light and Hydro One commented that the Transient Cyber Asset definition needs clarification regarding electronic access control and physical access control. The SDT has chosen to focus the requirements to the assets that are to be connected to the BES Cyber Systems that provide BES reliability operating services, as well as those residing within the same ESP. The goal is to protect the systems that can have a direct impact on real-time operations.

Massachusetts Municipal Wholesale Electric Company commented that the Transient Cyber Asset definition should not include examples. The SDT appreciates the comment. The SDT notes that other glossary terms use examples in the definitions. The SDT determined that the examples add clarity to assist the Responsible Entity in determining the scope and breadth of the term.

National Rural Electric Cooperative Association and Associated Electric Cooperative, Inc. commented that the Transient Cyber Asset definition is broad because directly connected could apply to any programmable device. The SDT added a clarification to the definition to indicate that Transient Cyber Assets are those devices "capable of transmittal of executable code" to the Cyber Assets and networks listed in the definition.

Removable Media

Southwest Power Pool Regional Entity commented that the certain portable media, such as external hard drives, should not be considered Removable Media and suggested clarification in the name of the term. The SDT appreciates the comment but determined that external hard drives should be included in the Removable Media definition. The SDT reasons that any media capable of introducing malicious software to the BES Cyber System should be subject to the appropriate requirements.

Edison Electric Institute, NiSource, We Energies, PNM Resources Resources, Oncor, Empire District Electric Company, ISO/RTO SRC, Seattle City Light, Large Public Power Council, Massachusetts Municipal Wholesale Electric Company, and American Public Power Association commented that the Removable Media definition is not consistent with the Transient Cyber Asset definition because it does not clarify to what the Removable Media is connected. Duke Energy and MidAmerican Energy Company suggested adding the three items listed in the Transient Cyber Asset definition as well as "directly connected" to the Removable Media definition. The SDT added "directly" in front of connected in the Removable Media definition and revised it to indicate that the device is "capable of the transmittal of executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset," which is similar to the Transient Cyber Asset definition. This makes the definitions consistent and gives clarity on the device's connection.

Seattle City Light, Large Public Power Council, Massachusetts Municipal Wholesale Electric Company, and American Public Power Association suggested that the SDT remove "portable media" from the definition because it may add confusion. Large Public Power Council and American Public Power Association suggested adding "capable of removal without powering down the system." The SDT removed "portable" from the definition and added "capable of the transmittal of executable code" to the definition.

Southern Company and Oncor suggested that the Removable Media definition be more specific to higher risk forms of media and other diagnostic devices. The SDT reasons that any media capable of introducing malicious software to BES Cyber Systems should be subject to the appropriate requirements. Each type of Removable Media has an element of risk and should be reviewed.

Southern Company and Oncor commented that the Removable Media definition states that a Cyber Asset is not Removable Media but that the Transient Cyber Asset definition does not explicitly exclude Removable Media. The SDT appreciates the comment but notes that because a Transient Cyber Asset is a Cyber Asset, Removable Media cannot be a Transient Cyber Asset because it is not a Cyber Asset.

Kansas City Power & Light commented that the Removable Media definition needs clarification regarding electronic access control and physical access control. The SDT has chosen to focus the requirements to the assets that are to be connected to the BES Cyber Systems that provide BES reliability operating services, as well as those residing within the same ESP. The goal is to protect the systems that can have a direct impact on real-time operations.

ISO/RTO SRC commented that the SDT should include tape as an example of Removable Media. The SDT considered the addition of tape as an example of Removable Media; however, determined that tape systems are not traditionally connected directly to BES Cyber Systems.

ISO/RTO SRC commented that the SDT should clarify if "A Cyber Asset is not Removable Media" is trying to say that Removable Media are not a Cyber Assets. The SDT revised the language to read "Removable Media are not Cyber Assets."

ISO/RTO SRC questioned whether Removable Media need to comply with additional requirements once they have been connected longer than 30 days. The SDT considers any portable media connected for more than 30 days to be part of the BES Cyber System.

American Electric Power requested clarity on why Transient Cyber Assets are associated with Removable Media in the standard. The SDT moved the language in the requirements to an attachment and separated the elements applicable to Transient Cyber Assets from those elements applicable to Removable Media.

Other

PacifiCorp, South Carolina E&G, Georgia Transmission Corporation, National Rural Electric Cooperative Association, and Pacific Gas & Electric suggested the SDT revise CIP-010-2, Requirement R4.

PacifiCorp recommended that the SDT revise the applicability columns in CIP-010-2, Requirement R4, Table 1 to include Transient Cyber Assets and Removable Media. The tables supporting CIP-010-2 Requirement R4, have been eliminated and the elements of a plan for Transient Cyber Assets and Removable Media has been moved to an attachment.

PacifiCorp, Georgia Transmission Corporation, National Rural Electric Cooperative Association, and South Carolina Electric & Gas commented that part 4.1 would be administratively burdensome. The SDT agrees and has modified its approach in CIP-010-2.

Georgia Transmission Corporation commented that the SDT should not borrow from medium impact requirements for transient devices. The SDT agrees and has modified its approach in CIP-010-2.

South Carolina SG&E commented that personnel with high and medium impact BES Cyber Systems access should not need additional authorizations and that entities should be able to designate personnel who can supervise unauthorized maintenance personnel (similar to NIST 800-53 MA-5). The SDT clarifies that users may be authorized by group in the plan(s) for Transient Cyber Assets and Removable Media. Therefore, an entity may choose to list an authorized user group as those that already have been authorized for access to high and medium impact BES Cyber Systems.

Pacific Gas & Electric commented that Requirement R4 should be required across all components within the ESP regardless of classification. In response, the SDT maintains that the requirements are targeting those BES Cyber Systems that have a direct impact on the BES.

Pacific Gas & Electric commented that user authorization should be by individual and not by group. The SDT appreciates the comment but notes that it is important to give entities the flexibility to capture authorization by group. For example, an entity may choose to list an authorized user group as those that already have been authorized for access to high and medium impact BES Cyber Systems. This eliminates redundancy of individual user authorization but ensures entities designate users of entity-owned or managed Transient Cyber Assets.

ACES commented that it is supportive of the revisions as long as RAI is fully implemented by the effective date. The SDT refers ACES to the question 5 comment response.

MRO NERC Standards Review Forum commented that CIP-002-5.1 should be updated with the new and revised definitions. The SDT appreciates the comments but is not revising CIP-002-5.1 at this time. The scope of the SDT's Standards Authorization Request (SAR) is focused on the directives contained in FERC Order No. 791. Therefore, the SDT revised only those standards that should include language addressing the directives.

Question 5: Identify, Assess, and Correct

5. *The SDT removed the Identify, Assess, and Correct (IAC) language from 17 requirements to meet the directive in FERC Order No. 791 to remove or modify the IAC language. Do you support this revision approach? If not, why not and what alternative approach do you recommend?*

Support Removal

Dominion, Bonneville Power Administration, Public Service Enterprise Group; MidAmerican Energy Company, CenterPoint Energy, ACES Members, MRO NERC Standards Review Forum, Edison Electric Institute; Seattle City Light, Peak Reliability, Florida Municipal Power Authority, Large Public Power Council, Southern Company, NiSource, IESO, Southern California Edison Company, Tacoma Public Utilities, PNM Resources Resources, Kansas City Power & Light, Exelon Companies, American Public Power Association, National Rural Electric Cooperative Association, Oncor, The Empire District Electric Company, and Southwest Power Pool Regional Transmission Organization supported the removal of the IAC language. In response, the SDT thanks those entities for their comments.

Oppose IAC Removal

Portland General Electric, Nebraska Public Power District, City of Tallahassee, Tri-State G & T, and Idaho Power commented that the inclusion of this language in the CIP Version 5 standards was a large part of the reason that the industry voted to pass the standards in the first place and that the directive allowed for a modification of the IAC language. The SDT appreciates the concerns raised with the removal of IAC. However, the majority of stakeholders indicated a preference in removing the IAC language to address the FERC directive. NERC continues to develop Reliability Assurance Initiative (RAI) to address the compliance concerns that IAC sought to address. The comments opposing the removal of IAC and the underlying compliance concerns that remain are being forward to NERC Compliance.

Modify IAC/Standard Language

Dominion commented that an alternative approach to RAI would be to address FERC's concerns by modifying the individual Parts of each of the CIP Requirements. The SDT appreciates the suggestions to modify the IAC language to meet the FERC Directive. However, the majority of stakeholders indicated a preference in removing the IAC language to address the FERC directive.

Southwest Power Pool Regional Entity suggested that a performance metric could be developed that allowed for an infrequent (frequency to be defined) occurrence as long as the entity's detective controls detected the unauthorized implementation activity within a to-be defined detection period (perhaps 24 hours) and the unauthorized change was promptly investigated. In response, the Cyber Security Order 706 SDT previously explored incorporating performance metrics into the requirements, but the approach proved problematic by triggering a new host of questions related to the metric. As a consequence, the requirement lost focus on the real intent of the security measure. The IAC language attempted to balance the security objective with reasonable compliance expectations. At present, NERC continues to develop RAI to address the compliance concerns that IAC sought to address. The comments received on IAC are being forwarded to NERC Compliance. Performance or qualitative metrics may have a useful role under the RAI program whether as part of a risk assessment methodology or other element.

Portland General Electric commented that it would be worthwhile to modify the language to add a qualitative aspect to address zero tolerance concerns, and Occidental Chemical Corporation suggested to encode the IAC concept into separate sub-requirements under each of the affected requirements. The SDT appreciates the

comments on including a qualitative aspect and IAC in a different structure in the language. During development, the SDT explored options in the requirement language to address the zero defect concern rather than just removal of IAC. Ultimately, the SDT determined that this additional language did not provide clarity on performance obligations in the requirement and did not address zero tolerance concerns. The SDT noted that NERC continues to develop RAI to address the compliance concerns that IAC sought to address. The comments opposing the removal of IAC and the underlying compliance concerns that remain are being forward to NERC Compliance.

Liberty Electric System commented that, at a minimum, the VSLs and Measures should be rewritten to allow for minor instances of errors. For example, instead of a single instance of failing to revoke access for a transfer, rewrite the requirement to require a process that assures the access is revoked, with a low violation if the process fails to keep instances under 5% annually, or less than two in cases where there are small numbers of transfers each year. Tampa Electric Co. expressed a similar comment to modify the VSLs for a future revision. In response, the SDT notes that VSLs define the degree to which compliance with a requirement was not achieved. The SDT states that RAI is the appropriate mechanism to address the zero tolerance concern.

Idaho Power stated that more work should be done to see if there is a way to fix the IAC language prior to it be discarded. In response, the SDT is supportive of the removal of the language as the IAC paradigm will be addressed in RAI.

Tri-State G&T suggested defining IAC as one defined term instead of three separate words. The entity further commented to change “deficiencies” to “possible violations.” In response, the CMEP program, from the auditing and enforcing perspective, handles possible violations and it is not appropriate for reference to violations to reside within the Requirement language itself.

Clarify RAI and Compliance

Pacific Gas & Electric commented that defining clearer requirements, scope definitions and obligations in the NERC Compliance Monitoring and Enforcement Program. In response, the comments relative to RAI and other compliance concerns are being forwarded to NERC. The SDT will emphasize the concerns about RAI implementation timing.

Tennessee Valley Authority requested clarity on the RAI process regarding reporting timeframe and definition of “minimal risk.” In response, NERC notes that assessment of risk is based on facts and circumstances. For a more detailed explanation of assessing risk and the factors to consider in the assessment, NERC encourages entities to refer to the Self-Report User Guide, located here. Also, NERC has posted more than 1,100 minimal risk CIP FFTs on its webpage to provide Registered Entities with information on what constitutes minimal risk and how to mitigate minimal risk noncompliance.

Bonneville Power Administration commented that a lack of clearly defined measures results in inconsistent audit approaches and findings. In response, NERC notes that NERC and the Regional Entities have developed the ERO Enterprise Compliance Auditor Manual and Handbook and the ERO Auditor Checklist to define techniques, tools, and methods to perform compliance monitoring in a consistent manner. The ERO Enterprise is hosting training webinars prior to full implementation in the fourth quarter of 2014.

Idaho Power stated that industry is left with no time frames or guarantees of what RAI will become or when it is implemented. Nebraska Public Power District stated that RAI is an enforcement mechanism and not a compliance action. In response, NERC notes that several RAI projects have begun implementation in 2014, including the user guides, triage process, compliance exceptions, and aggregation of minimal risk issues programs. Development of the compliance monitoring-related programs is underway for implementation in 2015. The lessons learned from the development and early implementation of these programs will inform a filing to FERC in the fourth quarter of 2014. A current timeline and description of RAI activities is available on the RAI webpage, located here. The

aggregation of minimal risk issues and compliance exceptions are the two programs most relevant to these Standards. With aggregation, select Registered Entities[2] may track their minimal risk noncompliance without having to submit a Self-Report for each failure to comply with a Requirement. Such noncompliance would presumably be treated as a compliance exception. A compliance exception is a minimal risk noncompliance that is mitigated or can be mitigated within one year. Compliance exceptions do not become Possible Violations and do not initiate an enforcement process.

Peak Reliability suggested that concrete threshold reporting criteria for certain Requirements should be set. The SDT has chosen not to set such concrete threshold reporting criteria in the Requirements.

ISO/RTO SRC asked when will industry see a specific description of the RAI program as applied to CIPv5 standard compliance enforcement and expectations of RE's for collecting evidence to support the RAI process. In response, NERC conducted a joint webinar on June 19 for both the CIP Version 5 revisions activity and the RAI program. NERC will look into conducting something similar in the future and is continuing outreach on the RAI program.

Kansas City Power & Light commented that this concept would be addressed in tools and frameworks accomplished through the RAI, however, consistency in auditor training and approach will be critical to the success of the RAI program. In response, NERC agrees with the importance of auditor training and RAI components are a crucial aspect of the ERO training now and going forward.

Clarify RAI Prior to Implementation or Final Ballot

Public Service Enterprise Group commented that it would like to have additional clarity and finalization of the RAI process prior to the implementation of the new standard language. In response, the SDT understands that RAI is one of the biggest goals of the ERO. NERC's continued outreach on RAI will help alleviate industry's concerns. ACES Members are supportive of the approach as long as RAI is fully implemented.

MidAmerican and NV Energy stated that NERC can support the SDT efforts by implementing compliance exceptions prior to the second or final ballot. In response, NERC notes that it began implementation of the compliance exceptions program as of November 2013 for select Registered Entities. Eligibility expanded to additional Registered Entities in May 2014, and compliance exception treatment will be available January 1, 2015 to all Registered Entities for minimal risk noncompliance discovered through any method.

Need to address zero tolerance

Dominion, Southwest Power Pool Regional Entity, Bonneville Power Administration; Portland General Electric, Public Service Enterprise Group, We Energies, Occidental Chemical Corporation, Liberty Electric Power LLC, Idaho Power, City of Tallahassee, NV Energy; Nebraska Public Power District, Edison Electric Institute, Florida Municipal Power Authority, Large Public Power Council, ISO/RTO SRC, Southern Company, NiSource, Tacoma Public Utilities, Xcel Energy, PNM Resources Resources, and Oncor commented that the zero tolerance issue needs to be addressed. In response, while the removal of the IAC language returns the requirements to a zero tolerance construct, NERC committed to alleviate the zero tolerance concerns through the implementation of the RAI compliance approach (see the Q4 response and others in the FAQs document). In response, the comments relative to compliance concerns will be forwarded to the NERC Compliance department.

Other

American Public Power Association encouraged the SDT to provide guidance to NERC staff on the development of the proposed RSAWs. In response, while the SDT is not part of the RSAW development team, the SDT submitted

[2] The Enforcement Activities Overview, available on the RAI webpage, contains further details on eligibility for the aggregation program.

team comments on the RSAWs posted for comment during the initial comment period. The SDT continues to engage with the RSAW development team to provide input on the RSAWs.

Question 6: Implementation Plan

6. *The Implementation Plan uses the existing effective date of the FERC approved CIP V5 Standards for CIP-003-6 Requirement R2 and provides additional time for compliance for CIP-006-6, Requirement R1, Part 1.10; CIP-007-6, Requirement R1, Part 1.2; and CIP-010-2, Requirement R4. Are the timeframes reasonable and appropriate? If not, please explain.*

CIP-003-6

Duke Energy, Nebraska Public Power District, American Public Power Association, and Bonneville Power Administration suggested a later enforcement date, specifically that the low impact requirements should be enforceable one year later (January 1, 2018). American Public Power Association suggested that the implementation plan should call out two years after FERC approval or April 1, 2017, whichever is later for compliance. In response, the SDT understands the additional specification for Requirements applying to low impact BES Cyber Systems requires additional resources for implementation. In weighing the specificity with the already approved deadline of April 1, 2017, the SDT proposes an implementation plan which considers both the effort of implementation and the general impact to the BES. Requirements that entities can implement organizationally retain the same date of April 1, 2017. These Requirements include cyber security policy, awareness, and incident response plan. The physical and electronic access Requirements have obligations which generally necessitate deployment of technical controls. For these, we have graduated the implementation based on the technical controls. This approach balances the objective to implement on a similar schedule as CIP-003-5 with the additional effort to meet the new specific Requirements.

Similar to the comments above, Exelon Companies commented that the implementation plan should allow at least a year from the effective date of CIP-003-6. The Implementation Plan should make it clear that CIP-003-6, Requirement R2 will replace CIP-003-5 Requirement R2. In response, in addition to the SDT's response above, CIP-003-5 is retired with the implementation of CIP-003-6 and the Requirement applying to low impact BES Cyber Systems will be replaced as suggested.

CIP-006-6/CIP-007-6

Southwest Power Pool Regional Entity commented that the implementation plan for CIP-006-6, Requirement R1, Part 1.10 should be consistent with the actual Version 3 expectation and that additional time is not needed for CIP-007-6 Requirement R1, Part 1.2. In response, the Implementation Plan for CIP-006-6 Requirement Part 1.10 does consider the version 3 expectation and only provides additional time "for new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3". Regarding CIP-007-6, the additional 9 months may be necessary depending on how entities disable physical ports. This is an additional effort on top of what is necessary to implement version 5. For large control centers, this may require additional inventory work to ensure nonprogrammable components meet this Requirement.

Southwest Power Pool Regional Transmission Organization recommended that the six-month window for CIP-007-6 R1, Part 1.2 be extended to a nine-month window, reducing the number of dates and outlying requirements. In response, the additional requirements in CIP-006-6 and CIP-007-6 now have the same additional 9 months for compliance.

CIP-010-2

CenterPoint Energy stated that the timeframe for CIP-010-2 Requirement R4 is not appropriate, and recommended that Registered Entities not be required to comply with Reliability Standard CIP-010-2,

Requirement R4 until at least one year after the effective date of Reliability Standard CIP-010-2. In response, the SDT notes that the implementation period for CIP-010-2 Requirement R4 calls for nine calendar months after the effective date of CIP-010-2 which allows entities enough time to prepare for compliance based on SDT discussion of all the implementation compliance dates for modified requirements.

Southwest Power Pool Regional Entity commented that CIP-010-2 Requirement R4 does not need nine additional months. In response, this Requirement has been modified and the additional time is necessary for entities to develop and implement their plan(s) to address transient devices.

Overall Implementation

Colorado Springs Utilities, Tennessee Valley Authority, Western Area Power Administration, and Salt River Project recommended changing the Implementation Plan time schedule to fall after the CIP Version 5 standards implementation dates. In response, the SDT states that the implementation plan is drafted to account for the Version 5 Standards as suggested. The Version 5 effective dates are used as the minimum bound for Version 5 Revisions. This ensures a seamless transition across versions on April 1, 2016 and April 1, 2017. Additional time beyond the version 5 effective dates is given for all but the Requirements in which the IAC language was removed. The IAC removal does not provide any additional obligations to Responsible Entities.

City of Tallahassee commented that FERC should issue an order to extend the effective date at least another full six months for each standard/requirement for which a modification to the language was made. In response, additional time beyond the version 5 effective dates is given for all but the Requirements in which the IAC language was removed. The IAC removal does not provide any additional obligations to Responsible Entities.

Exelon Companies commented that the Implementation plan uses “months” and “calendar months” and requested clarity whether there is a difference between the two terms and, if no difference is intended, suggested to use one for consistency. In response, the SDT has modified the Implementation Plan to address this inconsistency.

National Rural Electric Cooperative Association commented that not balloting the Implementation Plan separately was a violation of the Standards Processes Manual (SPM). In response, in section 4.4.3 of the SPM, “The implementation plan is posted with the associated Reliability Standard or Standards during the 45 (calendar) day formal comment period and is balloted with the associated Reliability Standard.” Therefore, the implementation plan was included as a component of the Reliability Standard comment period and ballot.

National Rural Electric Cooperative Association also requested that the SDT consider using the same additional time for compliance for all revised or new requirements under the current CIP V5 revision project. In response, the additional requirements in CIP-006-6 and CIP-007-6 now have the same additional nine months for compliance. The SDT has modified the Implementation Plan for low impact Requirements in response to other commenters.

Arkansas Electric Cooperative Corporation expressed support for addressing all four directive areas in the one-year timeframe. Arkansas Electric Cooperative Corporation went on to further comment that it is important to have industry-developed objective criteria for the low impact BES Cyber Systems when the requirements go into effect on April 1, 2017. The industry begins its 7th year in which these standards have been in development. It is difficult to grow and mature security programs with so much change in the compliance rules. Arkansas Electric Cooperative Corporation stated they hope the industry, NERC, and FERC can come to an agreement in the coming months and provide finality to these Reliability Standards for a time. The SDT thanks you for your comments.

Question 7: Canadian or Other Regulatory Requirements

7. *Are there any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.*

There were no commenters who responded to this question identifying any jurisdictional specific regulatory requirements.

Question 8: Other Areas Within SAR

8. *Do you have input on other areas, within the scope of the Standards Authorization Request, for the standards or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions.*

Low Impact

Tennessee Valley Authority requested clarification on the threshold for the low impact categorization and whether the BES definition establishes the lower boundary. In response, the Applicability section and Attachment 1, Section 3 of CIP-002-5.1 establishes the lower boundary, and while the BES definition is a basis for the lower boundary, it does not always establish it. The use of Facilities in the Applicability section ties back to the BES definition, but it is possible to have systems or equipment, such as Control Centers and systems or those critical to system restoration.

Southwest Power Pool Regional Transmission Organization sought clarification on the security awareness component of CIP-003-6. South Feather Power Project and Seattle City Light commented that the security awareness requirement should be annual instead of quarterly. The SDT has modified the language to "at least once every 15 calendar months" from "quarterly." In addition, the SDT removed the training component from CIP-003-6 because training is addressed in CIP-004-6.

Seattle City Light also suggested that the SDT change the presentation of the low impact controls, either by dispersing them throughout the other standards or creating a CIP-012-1. The SDT considered dispersing the low impact controls throughout the CIP standards but determined that they could not fit into the table format because the medium and high impact controls apply at the system level whereas the low impact controls apply at the asset containing low impact BES Cyber System level. The SDT also considered drafting CIP-012-1 to include low impact requirements. However, the SDT determined that it was more appropriate to keep the low impact policy requirement in CIP-003-6 because the policy requirements for high and medium impact were located there as well. To address comments on reorganizing low impact requirements, the SDT determined that it would put the low impact technical requirements into an attachment to CIP-003-6, Requirement R2, which requires a plan to address the elements in the attachment. In addition, the SDT placed the low impact policy requirement into CIP-003-6, Requirement R1 to consolidate the policy requirements for low, medium, and high impact into one requirement.

MidAmerican Energy Company also suggested adding "for its assets identified in CIP-002-5.1" into Requirement R2 to clarify the assets to which it applies. The SDT added "Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems" into Requirement R2 to clarify applicability.

Rayburn Country Electric Cooperative and Wisconsin Electric Power Company suggested the SDT develop guidance in CIP-003-6 to address compliance concerns. In response Rayburn County Electric Cooperative, see the comment response summary for Question 1. The SDT has provided more specific examples and guidance to the Requirement applying to low impact BES Cyber Systems. In response to Wisconsin Electric Power Company's concern that entities cannot go beyond the Requirement objective, the NERC Reliability Standards should not contain language about compliance and notes that the language included in the background sections of these standards may be inappropriate to include. The SDT may revisit the background sections of the standards at a later date.

American Public Power Association commented on compliance concerns and suggested a survey of entities to determine the administrative workload for the low impact requirements. In response, the SDT notes that NERC

will consider the need for a survey. If you have any information on this topic that would assist NERC, please submit them in your comments.

Exelon Companies and National Rural Electric Cooperative Association expressed support of getting the low impact requirements to a steady-state. The SDT continues to develop revisions to the low impact requirements in an effort to build consensus and gain approval prior to the February 3, 2015 FERC filing.

Revise CIP-002-5.1, CIP-005-5, and CIP-008-5

Edison Electric Institute, Tampa Electric Company, NiSource, and Nevada Energy suggested the SDT make conforming changes to CIP-002-5.1, CIP-005-5, and CIP-008-8 to maintain consistency throughout the CIP suite of standards. Southwest Power Pool Regional Entity submitted errata changes to the Guidelines and Technical Basis section of CIP-002-5.1. ISO/RTO SRC and Entergy recommended making all CIP standards version 6. Manitoba Hydro and Duke Energy suggested changing the effective dates of the Version 5 standards to make all consistent. Southern Company and Georgia Transmission Corporation requested clarification of "associated with" in CIP-002-5.1. Wisconsin Electric Power Company commented that Criterion 2.3 of CIP-002-5.1 Attachment 1 is not specific enough as to which BES Cyber Assets meet the criterion and recommended that CI-002-5.1, CIP-005-5, and CIP-008-5 clarify in guidance that those entities going above and beyond the requirements would not incur additional compliance obligations. Massachusetts Municipal Wholesale Electric Company suggested revising CIP-005-5 and CIP-008-5 to reference low impact BES Cyber Systems.

The SDT appreciates the comments regarding revisions to CIP-002-5.1, CIP-005-5, and CIP-008-5. At this time the SDT continues to focus on the four main directive areas from Order No. 791. As a result, the SDT will not revise CIP-002-5.1, CIP-005-5, and CIP-008-5 during this phase of development.

Reliability Standard Audit Worksheets (RSAWs)

Florida Municipal Power Agency (Florida Municipal Power Authority) requested that NERC run non-binding polls and post comments received on the RSAWs. Edison Electric Institute, Florida Municipal Power Authority, and First Energy commented that the CIP-002-5.1 RSAW expands beyond the scope of the standard. Florida Municipal Power Authority noted that the CIP-003 RSAW has the wrong number in 6a of Requirement 2.5. Edison Electric Institute and FirstEnergy emphasized that the SDT and the RSAW development team should continue coordination during the standards development. Exelon Companies commented that the RSAWs do not provide relief from zero tolerance concerns and suggested the RSAWs be revised and posted for industry comment during the next revisions to the standards.

The SDT coordinated with the RSAW development team during drafting activities and will continue this coordination for the next revisions. As part of this collaboration, the SDT will pass the comments received on the RSAWs to the RSAW development team.

Reliability Assurance Initiative (RAI)

Northeast Power Coordinating Council (Northeast Power Coordinating Council), Exelon Companies, and National Rural Electric Cooperative Association requested more scenarios as to how CIP requirements will work in the RAI context and suggested using the low impact or "identify, assess, and correct" (IAC) requirements to demonstrate RAI concepts. Avista and National Rural Electric Cooperative Association commented that RAI should be finalized prior to final ballot.

The SDT appreciates the comments regarding RAI and recognizes the relationship between the removal of IAC language and RAI. The SDT continues its coordination with NERC staff on RAI and will pass on these and other relevant comments to NERC staff involved in the development of RAI.

Other Comments

Northeast Power Coordinating Council and Hydro One commented that the SDT should be able to help clarify issues discovered during the CIP Version 5 Implementation Study, particularly on the transfer trip issue, programmable devices definition, and clarification on "effect within 15 minutes." The SDT appreciates these comments but continues to focus effort on the four main directive areas from FERC Order 791. NERC has employed an industry stakeholder group to review and provide guidance toward these issues outside of the standards setting process.

Northeast Power Coordinating Council and Hydro One suggested adding "or" to CIP-010-2, Requirement R4, Part 4.1.4 to make it consistent with Requirement R1, Part 1.1.1. The SDT proposes to revise Requirement R4 to have an attachment with the elements related to transient devices.

Pacific Gas & Electric requested guidance on how Electro Magnetic Pulse (EMP) anomalies should be considered in risk assessments or policies and procedures, and in response, the SDT notes the CIP Cyber Security Standards have the objective of protecting BES Cyber Systems against cyber security risks. EMP and other related threats associated with the BES and BES Cyber Systems are outside the scope of this SDT.

Southwest Power Pool Regional Entity commented that there is an inconsistency in the implementation plan for CIP-004-6 because six months is allowed if government authority is required and only three months is allowed if government authority is not required. In response, this has been corrected to allow three calendar months after approval by a government authority.

PacifiCorp agrees with the communication networks revisions and does not recommend further edits. The SDT appreciates the comment and PacifiCorp's support of the revisions.

Dynegy requested that the webinars on the SDT's revisions and on RAI be posted to the website. The SDT's webinar and slides may be found here and here. The RAI webinar and slides may be found here and here.

Western Area Power Administration requested clarity on the object of the standards and align them with the risk to the BES so auditors and entities have a consistent approach. The SDT appreciates these comments but notes the rapidly changing and variant cyber security risk profile across the BES make this approach particularly unsuitable for Reliability Standards development. The approach is to develop standards for cyber security controls that address a wide set of common cyber security vulnerabilities.

Manitoba Hydro noted that the Compliance Enforcement Authority (CEA) definition is incorrect in Section C1.1 of the standards because Public Utility Board is its CEA. In response, the purpose of the compliance section of the standard is to describe the CEA's activities. If a province in Canada is not subject to the ROP provisions related to the CMEP and has its own enforcement, then these provisions simply would not apply.

Exelon Companies requested more guidance language be developed to support the requirements. The SDT appreciates the comment and will draft guidance language to support the proposed Requirements and additional revisions.

Texas Reliability Entity commented that entities should be required to demonstrate evidence of the effective execution of controls and not just that they have a policy or procedure. The SDT appreciates the comment and notes that the "implement" term in the requirements means that entities should execute the performance requirements and provide documentation of the implementation.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *policy* refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of *policies* also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save

the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity; and

1.2.4. Cyber Security Incident Response

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

The requirement to implement a cyber security plan for assets containing low impact BES Cyber Systems provides a minimum set of cyber security controls for assets containing low impact BES Cyber Systems. Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised. To that end, Requirement R2 requires Responsible Entities to implement documented cyber security plans covering four subject matter areas – (1) cyber security awareness, (2) physical access controls, (3) electronic access controls, and (4) cyber security incident response. In response to directives in FERC Order No. 791, Requirement R2 provides for the specific elements that must be included in the cyber security plan(s). Attachment 1 provides these elements. These plans, along with the cyber security policies required under Requirement R1, Part 1.2, provide sufficient operational, procedural, and technical safeguards for assets containing low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the Bulk-Power System, Attachment 1 provides Responsible Entities flexibility on how to apply the required security controls. Additionally, the SDT recognizes that many Responsible Entities have multiple impact rated BES Cyber Systems and has provided the ability to use high and medium impact BES Cyber System policies, procedures, and processes to implement the objective criteria within Attachment 1.

Responsible Entities will utilize their list of assets that contain low impact BES Cyber System(s) that is created as a result of applying CIP-002 to substantiate the sites or locations associated with low impact BES Cyber Systems. However, there continues to be no compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the elements in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the elements in Attachment 1 and additional evidence to demonstrate implementation of cyber security plan(s). Additional examples of evidence per element are located in Attachment 2.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior

Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-6, Requirement R2, Attachment 1, element 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-6, Requirement R2, Attachment 1, element 1. (R2) OR The Responsible Entity documented one or more incident response plans	The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented the determination of	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2)	within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security	whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for Low Impact External Routable Connectivity, but failed to establish a Low Impact Electronic Access Point, or permit inbound and outbound access and deny all other access, or other electronic access controls that provide	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center	equal or greater level of protection according to CIP-003-6, Requirement R2, Attachment 1, element 3. (R2) OR The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity that provides access to low impact BES Cyber Systems according to CIP-003, Requirement R2, Attachment 1, element 3. (R2) OR The Responsible Entity documented the physical	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, element 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical access controls according to CIP-003-6, Requirement R2, Attachment 1, element 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low	access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical access controls according to CIP-003, Requirement R2, Attachment 1, element 2. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, element 3. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-003-6 - Attachment 1

Required Elements for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the elements provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

1. Cyber security awareness: Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:

- Direct communications (for example, e-mails, memos, computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

2. Physical access controls: Each Responsible Entity shall implement controls to restrict physical access to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Low Impact BES Cyber System Electronic Access Point, if any, based on need as determined by the Responsible Entity, through one or more of the following:

- Access controls;
- Monitoring controls; or
- Other operational, procedural, or technical physical security controls.

3. Electronic access controls: Each Responsible Entity shall implement controls to restrict electronic access for Low Impact External Routable Connectivity and Dial-up Connectivity, which shall include the following, or other electronic access controls that provide an equal or greater level of protection:

3.1 For any Low Impact External Routable Connectivity, establish a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all other access; and

3.2 Authentication of all Dial-up Connectivity that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

4. Cyber Security Incident response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents.

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals.

4.4 Incident handling for Cyber Security Incidents.

4.5 Testing the Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident.

4.6 Record retention related to Reportable Cyber Security Incidents.

4.7 Updating the Cyber Security Incident response plan within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIP-003-6 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Element 1: An example of evidence for element 1 may include, but is not limited to documentation that the reinforcement of cyber security practices once every 15 months has been provided through dated copies of the information used to reinforce security awareness via direct communications, indirect communications or management support and reinforcement.

Element 2: Examples of evidence for element 2 may include, but are not limited to:

1. Documentation of one or more access controls (e.g. card key, special locks), monitoring controls (e.g. alarm systems, human observation), or other operational, procedural or technical physical security controls to restrict physical access to both:
    a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
    b. The Cyber Asset, if any, containing the Low Impact BES Cyber System Electronic Access Point.
2. Documentation showing that the physical access restrictions cited above are based on need, which may include, but is not limited to, a policy describing the high level operational or business need(s) for physical access.

Element 3: Examples of evidence for element 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections (e.g. IP addresses, ports, services) for any Low Impact BES Cyber System Electronic Access Point are confined to only those the Responsible Entity deems necessary; and documentation of authentication for Dial-up Connectivity (e.g. dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, access control on the BES Cyber System); or
- Documentation of other electronic access controls that provide an equal or greater level of protection.

Element 4: An example of evidence for element 4 may include, but is not limited to, dated documentation such as policies, procedures or process documents of one or more Cyber Security Incident response plan(s); either by asset or group of assets that include the following processes:

1. to identify, classify and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);

2. the identification and documentation of the roles and responsibilities for Cyber Security Incident response by groups of individuals (e.g. initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g. containment, eradication, recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to retain records related to Reportable Cyber Security Incidents (e.g. security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes).

Also include dated revised Cyber Security Incident response plan(s) that identify that the plan(s) were updated within 180 calendar days after a completion of a test or actual Reportable Cyber Security Incident.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. If a Responsible Entity has any high or medium impact BES Cyber Systems, the cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1.1. If a Responsible Entity has any assets from CIP-002 containing low impact BES Cyber Systems, the cyber security policy must cover in sufficient detail the four topical areas required by Requirement R1.2. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1. For Responsible Entities that have multiple impact rated BES Cyber Systems, they are not required to create separate cyber security policies for high or medium and low impact BES Cyber Systems. Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program

of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident

- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

Using the list of assets from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses the protection of all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), not an individual device or system level.

There are four main areas detailed in Attachment 1 that must be covered by this plan: cyber security awareness, physical security, electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity, and cyber security incident response.

Requirement R2 Attachment 1

Attachment 1 contains the elements that must be in the cyber security plan(s). The SDT's intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems and not maintain two separate programs. Guidance for each of the 4 subject matter areas of Attachment 1 is provided below.

Requirement R2 Attachment 1 – Security Awareness

The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. It is up to the entity as to the topics and how it schedules these topics. The Responsible Entity should be able to produce the awareness material that was delivered and the delivery method(s) (posters, emails, topics at staff meetings, etc.) that were used. The SDT does not intend that the Responsible Entity must maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be used in the program. Appropriate physical security topics (e.g. tailgating awareness and protection of badges for physical security, "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2 Attachment 1 – Physical Security

The Responsible Entity must document and implement controls to restrict physical access to the low impact BES Cyber Systems at a BES asset and Low Impact BES Cyber System Electronic Access Points (LEAP) (see Electronic Access Controls section below). If the LEAP is located within the BES asset and inherits the same controls outlined in element 2, this can be noted by the Responsible Entity to avoid duplicate documentation of the same controls. If the LEAP is located at another location, possibly a location without any BES Cyber Systems, then separate documentation and implementation of the physical security controls of the LEAP are required.

The Responsible Entity has flexibility in the controls used to restrict physical access to low impact BES Cyber Systems at a BES asset using one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users are not required.

The objective is to restrict physical access based on need and the need can be established at the policy level based on higher level operational or business needs for access to the site or systems. The SDT intent is that this need at the higher level be documented such that the requirement cannot be interpreted to mean that any and all access must be restricted. The

requirement does not imply that a specific business need must be documented for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (i) alarm systems to detect motion or entry into a controlled area, or (ii) human observation of a controlled area. Monitoring does not imply logging and maintaining logs, but monitoring that physical access has occurred or been attempted (e.g., door alarm or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity's controls.

Requirement R2 Attachment 1 – Electronic Access Controls

Where Low Impact External Routable Connectivity (LERC) or Dial-up Connectivity exists, the Responsible Entity must document and implement controls that include the LERC and Dial-up Connectivity to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. Two glossary terms are included in order to help clarify and simplify the language in Attachment 1. The SDT's intent in creating these terms is to avoid confusion with the similar concepts and requirements (ESP, EAP, ERC, EACMS) needed for high and medium impact BES Cyber Systems by utilizing separate terms that apply only to assets containing low impact BES Cyber Systems.

> **Low Impact External Routable Connectivity (LERC)** – includes any bi-directional routable protocol based connectivity between low impact BES Cyber Systems within a BES asset and Cyber Assets outside the BES asset containing the low impact BES Cyber Systems. The SDT, in order to avoid future technology issues, is specifically excluding from the definition direct Intelligent Electronic Device (IED) to IED communication used for protection and/or control between low impact BES Cyber Systems at different BES assets, such as IEC 61850 messaging. The SDT does not intend for the requirement to have an electronic access point even though there is LERC or to preclude the use of such time-sensitive (for example 4 ms or less) reliability enhancing functions if they use a routable protocol in the future.
>
> **Low Impact BES Cyber System Electronic Access Point (LEAP)** – is the interface on a Cyber Asset that allows and controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on a firewall, the internal interface on a router that has implemented an access control list (ACL), or an internal interface on a unidirectional gateway that physically enforces outbound-only data flows. LEAP are not to be considered EACMS or meet EACMS specific requirements (as utilized for the Electronic Security Perimeter protecting high and medium impact BES Cyber Systems). However they are required, as per element 2 of the cyber security plan elements, to have physical security controls. The location of the LEAP is not prescriptive and does not have to reside at the BES asset containing low impact BES Cyber Systems. This flexibility is included so that the standard does not require a unique LEAP per BES asset. Responsible Entities can have a single LEAP that controls the LERC from more than one BES asset containing low impact BES Cyber Systems. However the LERC between assets "behind" the LEAP and another asset containing a low impact BES Cyber

System must also pass through the single LEAP. Locating the LEAP at an external location with multiple BES assets containing low impact BES Cyber Systems "behind" it should not allow unfettered access from one BES asset to all other BES assets sharing the LEAP. It is also not the intent of the SDT where low impact BES Cyber Systems do not have any LERC that additional connectivity be established nor that a LEAP be established.

The electronic access controls should address the risk of using the asset's LERC or Dial-up Connectivity to gain access to the low impact BES Cyber Systems. For LERC, a LEAP shall be implemented that permits only necessary inbound and outbound access and denies all other access.

Examples of sufficient access controls may include:

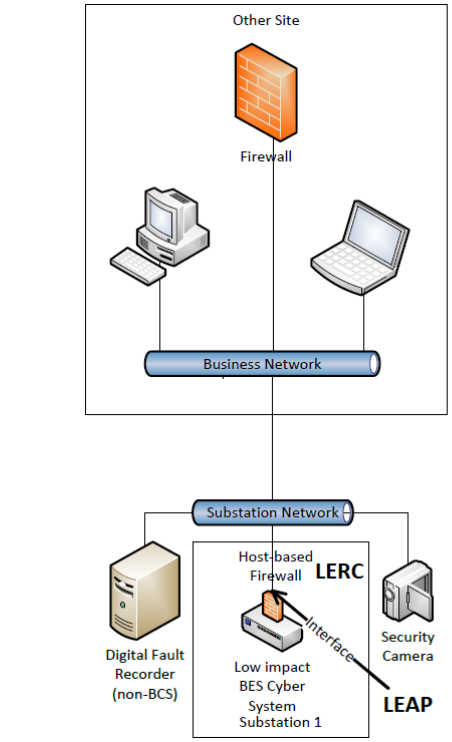
- Any LERC for the asset passes through a LEAP that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that the Responsible Entity deems necessary (e.g. IP addresses, ports, services) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.
- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no autoanswer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

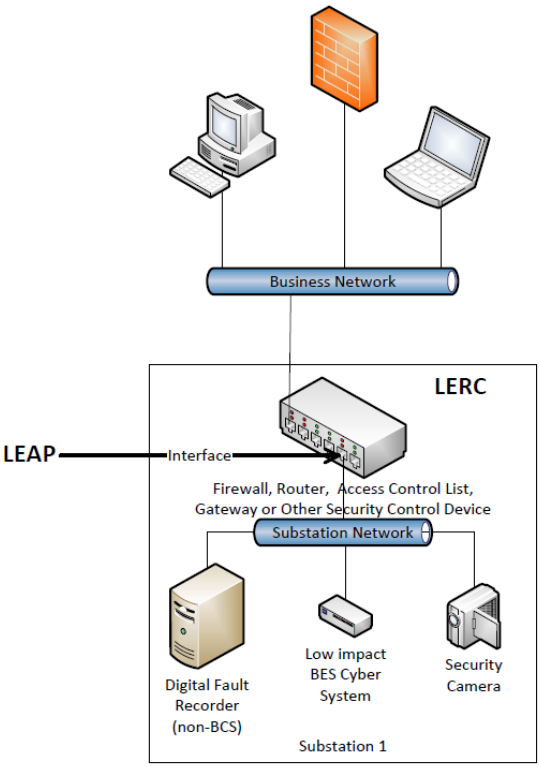
The SDT also notes it uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

The following diagrams explain the SDT's rationale.



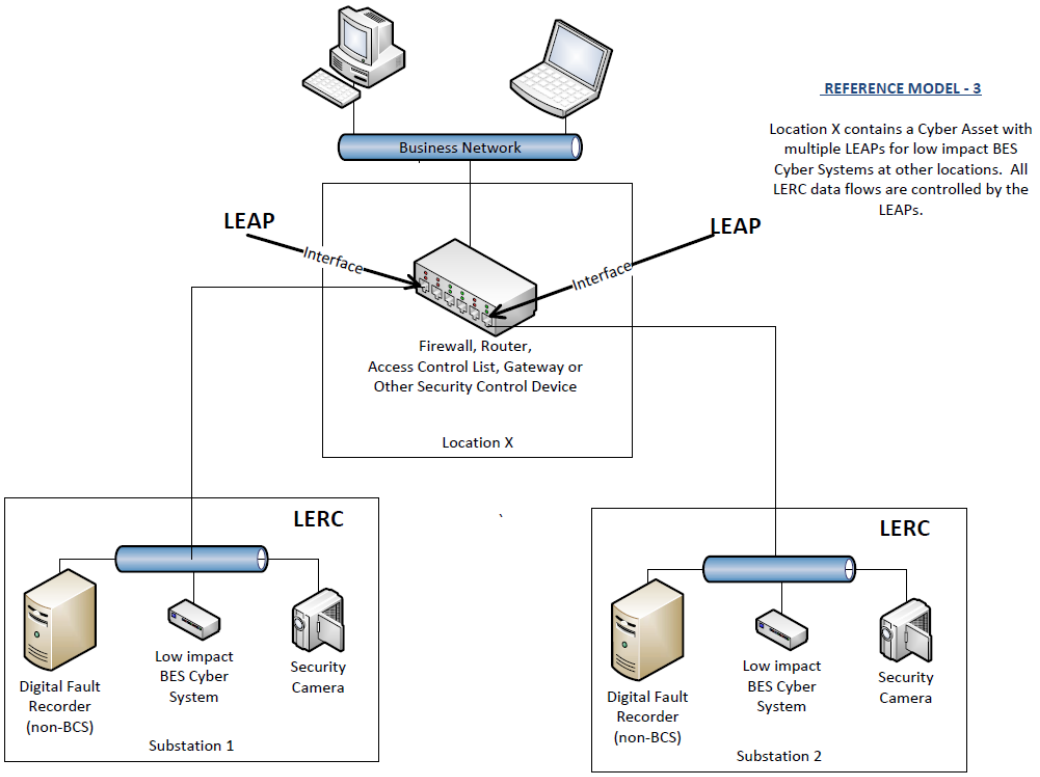
REFERENCE MODEL - 1

The low impact BES Cyber System is behind a LEAP. In this example, the LEAP is the network interface on the low impact BES Cyber System. The host-based firewall restricts electronic access for Low Impact External Routable Connectivity (LERC).



REFERENCE MODEL - 2

All LERC to the low impact BES Cyber System is controlled by an LEAP.



Requirement R2 Attachment 1 – Cyber Security Incident Response

The entity should have one or more documented cyber security incident response plans that include each of the topics listed. For assets that do not have LERC, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed. It is the intent of the SDT to have the cyber security incident response plan(s) kept current which includes updating the plan(s) within 180 days following a test or an actual incident.

In the event of a Reportable Cyber Security Incident, Attachment 1, element 4.6 specifies entities must retain relevant records for Reportable Cyber Security Incidents. Example evidence may include, but is not limited to, dated documentation, such as security logs, police reports,

emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes. Entities should refer to their handling procedures to determine the types of evidence to retain. The evidence retention period for records related to Reportable Cyber Security Incidents is defined in Section C.1.2 of this Standard, which is the same for all requirements in CIP-003-6.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R3:

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014

Description of Current Draft

This draft standard is being posted for an initial additional comment period and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-003-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *policy* refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of *policies* also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save

the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to ~~personnel who have authorized electronic access and/or authorized unescorted physical access to~~ its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity~~, for its high impact and medium impact BES Cyber Systems~~ shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

- **1.1.1.** Personnel and~~&~~ training (CIP-004);
- **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.1.3.** Physical security of BES Cyber Systems (CIP-006);
- **1.1.4.** System security management (CIP-007);
- **1.1.5.** Incident reporting and response planning (CIP-008);
- **1.1.6.** Recovery plans for BES Cyber Systems (CIP-009);
- **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
- **1.1.8.** Information protection (CIP-011); and
- **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

- **1.2.1.** Cyber security awareness;
- **1.2.2.** Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity; and

~~**1.1.9.**~~**1.2.4.** Cyber Security Incident Response

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

The requirement to implement a cyber security plan for assets containing low impact BES Cyber Systems provides a minimum set of cyber security controls for assets containing low impact BES Cyber Systems. Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised. To that end, Requirement R2 requires Responsible Entities to implement documented cyber security plans covering four subject matter areas – (1) cyber security awareness, (2) physical access controls, (3) electronic access controls, and (4) cyber security incident response. In response to directives in FERC Order No. 791, Requirement R2 provides for the specific elements that must be included in the cyber security plan(s). Attachment 1 provides these elements. These plans, along with the cyber security policies required under Requirement R1, Part 1.2, provide sufficient operational, procedural, and technical safeguards for assets containing low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the Bulk-Power System, Attachment 1 provides Responsible Entities flexibility on how to apply the required security controls. Additionally, the SDT recognizes that many Responsible Entities have multiple impact rated BES Cyber Systems and has provided the ability to use high and medium impact BES Cyber System policies, procedures, and processes to implement the objective criteria within Attachment 1.

Responsible Entities will utilize their list of assets that contain low impact BES Cyber System(s) that is created as a result of applying CIP-002 to substantiate the sites or locations associated with low impact BES Cyber Systems. However, there continues to be no compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users.

~~One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the~~

~~accountability and responsibility necessary for effective implementation of the standard's requirements by CIP Senior Manager approval of the policies specified in Part 2.1.~~

~~The language in Requirement R2, Part 2.4 "external routable protocol paths" and "Dial-up Connectivity" was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.4 uses the phrase "external routable protocol paths" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. The Standard Drafting Team (SDT) intent in using the phrase "external routable protocol paths" is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).~~

~~The additions to Requirement R2, in particular the processes required under Parts 2.2-2.6, address FERC Order No. 791 paragraphs 106-110, which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets. The SDT pulled language and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2.~~

~~In FERC Order No. 791 paragraphs 111-112, FERC upheld that creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.~~

R2. Each Responsible Entity ~~for its assets~~with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall ~~perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets*~~implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the elements in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the elements in Attachment 1 and additional evidence to demonstrate implementation of cyber security plan(s). Additional examples of evidence per element are located in Attachment 2. ~~Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table~~

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have external routable protocol paths.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance ~~Violation~~ Investigations

Self-Reporting

Complaints~~ Text~~

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate according to Requirement R1~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate according to Requirement R1~~ within 16 calendar months but did complete this approval in less than or equal to 17	calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate according to Requirement R1~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager ~~or delegate according to Requirement R1~~ within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as	calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES	identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or	months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16	more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-6, Requirement R2, Attachment 1, element 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-6, Requirement R2, Attachment 1, element 1. (R2) OR The Responsible Entity documented one or more incident	The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented the	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2) ~~The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) ~~The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2, Part 2.1. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its review of the one or more~~	response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for Low Impact External Routable Connectivity, but failed to establish a Low Impact Electronic Access Point, or permit inbound and outbound access and deny all other access, or other electronic access	~~the topics as required by Requirement R2, Part 2.1. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 18 calendar months of the previous review. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its approval of the one or more documented cyber~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according~~	Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2, Attachment 1, element 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing	controls that provide equal or greater level of protection according to CIP-003-6, Requirement R2, Attachment 1, element 3. (R2) OR The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity that provides access to low impact BES Cyber Systems according to CIP-003, Requirement R2, Attachment 1, element 3. (R2) OR	~~security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 18 calendar months of the previous approval. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not document or implement any processes for assets with a low impact rating to include the operational or procedural control(s) to restrict physical access as required by~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~to Requirement R2, Part 2.1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (2.1)~~ ~~OR~~ ~~The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.5. (2.5)~~ ~~OR~~ ~~The Responsible Entity did not~~	and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, element 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical access controls according to CIP-003-6, Requirement R2, Attachment 1, element 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical access controls according to CIP-003, Requirement R2, Attachment 1, element 2. (R2) ~~The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2, Part 2.1. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its review of the one or~~	~~Requirement R2, Part 2.2. (2.2)~~ ~~OR~~ ~~The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.3. (2.3)~~ ~~OR~~ ~~The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.4. (2.4)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~reinforce cyber security practices at least quarterly but did reinforce cyber security practices at least every two quarters. (2.6)~~ ~~OR~~ ~~The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.5 for assets with a low impact rating in less than or equal to 16 calendar months. (2.6)~~	containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, element 3. (R2) ~~The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2, Part 2.1. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its review of the one or more~~	~~more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 17 calendar months but did complete this approval in less than or equal to~~	~~OR~~ ~~The Responsible Entity did not implement any Cyber Security Incident response plans for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.5. (2.5)~~ ~~OR~~ ~~The Responsible Entity did not implement a security awareness program for assets with a low impact rating that collectively included the topics as required by Requirement R2, Part 2.6. (2.6)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (2.1)~~ ~~OR~~ ~~The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP~~	~~18 calendar months of the previous approval. (2.1)~~ ~~OR~~ ~~The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.3. (2.3)~~ ~~OR~~ ~~The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.4. (2.4)~~	~~The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced cyber security practices at least every 15 months. (2.6)~~ ~~OR~~ ~~The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced the topics within 18 calendar months as required by Requirement R2, Part 2.6. (2.6)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Senior Manager according to Requirement R2, Part 2.1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (2.1)~~ ~~OR~~ ~~The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.4. (2.4)~~ ~~OR~~ ~~The Responsible Entity implemented~~	~~OR~~ ~~The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include three of the topics as required by Requirement R2, Part 2.5. (2.5)~~ ~~OR~~ ~~The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include two of the topics as required by Requirement R2, Part 2.6. (2.6)~~ ~~OR~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.5. (2.5)~~ ~~OR~~ ~~The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include one of the topics as required by Requirement R2, Part 2.6. (2.6)~~ ~~OR~~	~~The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6)~~ ~~OR~~ ~~The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 for assets with a low impact rating in more than 17 calendar months but less than or equal to 18 calendar months. (2.6)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6)~~ ~~OR~~ ~~The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 in more than 16 calendar months but less than or equal to 17 calendar months. (2.6)~~		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified	The Responsible Entity has identified	The Responsible Entity has identified by name a	The Responsible Entity has not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (R4)	change in less than 50 calendar days of the change. (R4)		The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-003-6 - Attachment 1

Required Elements for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the elements provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

1. Cyber security awareness: Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:

- Direct communications (for example, e-mails, memos, computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

2. Physical access controls: Each Responsible Entity shall implement controls to restrict physical access to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Low Impact BES Cyber System Electronic Access Point, if any, based on need as determined by the Responsible Entity, through one or more of the following:

- Access controls;
- Monitoring controls; or
- Other operational, procedural, or technical physical security controls.

3. Electronic access controls: Each Responsible Entity shall implement controls to restrict electronic access for Low Impact External Routable Connectivity and Dial-up Connectivity, which shall include the following, or other electronic access controls that provide an equal or greater level of protection:

3.1 For any Low Impact External Routable Connectivity, establish a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all other access; and

3.2 Authentication of all Dial-up Connectivity that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

4. Cyber Security Incident response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents.

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals.

4.4 Incident handling for Cyber Security Incidents.

4.5 Testing the Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident.

4.6 Record retention related to Reportable Cyber Security Incidents.

4.7 Updating the Cyber Security Incident response plan within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIP-003-6 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Element 1: An example of evidence for element 1 may include, but is not limited to documentation that the reinforcement of cyber security practices once every 15 months has been provided through dated copies of the information used to reinforce security awareness via direct communications, indirect communications or management support and reinforcement.

Element 2: Examples of evidence for element 2 may include, but are not limited to:

1. Documentation of one or more access controls (e.g. card key, special locks), monitoring controls (e.g. alarm systems, human observation), or other operational, procedural or technical physical security controls to restrict physical access to both:
    a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
    b. The Cyber Asset, if any, containing the Low Impact BES Cyber System Electronic Access Point.
2. Documentation showing that the physical access restrictions cited above are based on need, which may include, but is not limited to, a policy describing the high level operational or business need(s) for physical access.

Element 3: Examples of evidence for element 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections (e.g. IP addresses, ports, services) for any Low Impact BES Cyber System Electronic Access Point are confined to only those the Responsible Entity deems necessary; and documentation of authentication for Dial-up Connectivity (e.g. dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, access control on the BES Cyber System); or
- Documentation of other electronic access controls that provide an equal or greater level of protection.

Element 4: An example of evidence for element 4 may include, but is not limited to, dated documentation such as policies, procedures or process documents of one or more Cyber Security Incident response plan(s); either by asset or group of assets that include the following processes:

1. to identify, classify and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);
2. the identification and documentation of the roles and responsibilities for Cyber Security Incident response by groups of individuals (e.g. initiating, documenting, monitoring, reporting, etc.);

3. for incident handling of a Cyber Security Incident (e.g. containment, eradication, recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to retain records related to Reportable Cyber Security Incidents (e.g. security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes).

Also include dated revised Cyber Security Incident response plan(s) that identify that the plan(s) were updated within 180 calendar days after a completion of a test or actual Reportable Cyber Security Incident.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. If a Responsible Entity has any high or medium impact BES Cyber Systems, ~~The~~ the cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1.1. If a Responsible Entity has any assets from CIP-002 containing low impact BES Cyber Systems, the cyber security policy must cover in sufficient detail the four topical areas required by Requirement R1.2. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1. For Responsible Entities that have multiple impact rated BES Cyber Systems, they are not required to create separate cyber security policies for high or medium and low impact BES Cyber Systems. Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program

of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel ~~&~~ and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident

- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~The~~ Using the list of assets from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses the protection of~~to outline a set of protections designed for~~ all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at an asset ~~programmatic~~ or site level (assets containing low impact BES Cyber Systems), not an individual device or system level.

There are four main areas detailed in Attachment 1 that must be covered by this ~~security program~~plan: cyber security awareness, physical security, electronic access controls for Low

Impact External Routable Connectivity and ~~for all external routable protocol paths or~~ Dial-up Connectivity~~, a security awareness program~~, and cyber security incident response ~~plans~~.

Requirement R2 Attachment 1

Attachment 1 contains the elements that must be in the cyber security plan(s). The SDT's intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems and not maintain two separate programs. Guidance for each of the 4 subject matter areas of Attachment 1 is provided below.

Requirement R2 Attachment 1 – Security Awareness

The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. It is up to the entity as to the topics and how it schedules these topics. The Responsible Entity should be able to produce the awareness material that was delivered and the delivery method(s) (posters, emails, topics at staff meetings, etc.) that were used. The SDT does not intend that the Responsible Entity must maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be used in the program. Appropriate physical security topics (e.g. tailgating awareness and protection of badges for physical security, "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2 Attachment 1 – Physical Security

The Responsible Entity must document and implement controls to restrict physical access to the low impact BES Cyber Systems at a BES asset and Low Impact BES Cyber System Electronic Access Points (LEAP) (see Electronic Access Controls section below). If the LEAP is located within the BES asset and inherits the same controls outlined in element 2, this can be noted by the Responsible Entity to avoid duplicate documentation of the same controls. If the LEAP is located at another location, possibly a location without any BES Cyber Systems, then separate documentation and implementation of the physical security controls of the LEAP are required.

The Responsible Entity has flexibility in the controls used to restrict physical access to low impact BES Cyber Systems at a BES asset using one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. User authorization programs and lists of authorized users are not required.

The objective is to restrict physical access based on need and the need can be established at the policy level based on higher level operational or business needs for access to the site or systems. The SDT intent is that this need at the higher level be documented such that the

requirement cannot be interpreted to mean that any and all access must be restricted. The requirement does not imply that a specific business need must be documented for each access or authorization of a user for access.

Monitoring as a physical security control can be used as a complement or an alternative to access control. Examples of monitoring controls include, but are not limited to: (i) alarm systems to detect motion or entry into a controlled area, or (ii) human observation of a controlled area. Monitoring does not imply logging and maintaining logs, but monitoring that physical access has occurred or been attempted (e.g., door alarm or human observation, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity's controls.

~~2.2 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.~~

~~2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity's controls.~~**Requirement R2 Attachment 1 – Electronic Access Controls**

~~2.4 – The~~ Where Low Impact External Routable Connectivity (LERC) or Dial-up Connectivity exists, the Responsible Entity must ~~have implemented processes~~document and implement controls that include the LERC ~~external routable protocol~~ and Dial-up ~~connectivity~~ Connectivity ~~paths~~ to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. Two glossary terms are included in order to help clarify and simplify the language in Attachment 1. The SDT's intent in creating these terms is to avoid confusion with the similar concepts and requirements (ESP, EAP, ERC, EACMS) needed for high and medium impact BES Cyber Systems by utilizing separate terms that apply only to assets containing low impact BES Cyber Systems.

> **Low Impact External Routable Connectivity (LERC)** – includes any bi-directional routable protocol based connectivity between low impact BES Cyber Systems within a BES asset and Cyber Assets outside the BES asset containing the low impact BES Cyber Systems. The SDT, in order to avoid future technology issues, is specifically excluding from the definition direct Intelligent Electronic Device (IED) to IED communication used for protection and/or control between low impact BES Cyber Systems at different BES assets, such as IEC 61850 messaging. The SDT does not intend for the requirement to

have an electronic access point even though there is LERC or to preclude the use of such time-sensitive (for example 4 ms or less) reliability enhancing functions if they use a routable protocol in the future.

Low Impact BES Cyber System Electronic Access Point (LEAP) – is the interface on a Cyber Asset that allows and controls the LERC. Examples include, but are not limited to, the internal (facing the low impact BES Cyber Systems) interface on a firewall, the internal interface on a router that has implemented an access control list (ACL), or an internal interface on a unidirectional gateway that physically enforces outbound-only data flows. LEAP are not to be considered EACMS or meet EACMS specific requirements (as utilized for the Electronic Security Perimeter protecting high and medium impact BES Cyber Systems). However they are required, as per element 2 of the cyber security plan elements, to have physical security controls. The location of the LEAP is not prescriptive and does not have to reside at the BES asset containing low impact BES Cyber Systems. This flexibility is included so that the standard does not require a unique LEAP per BES asset. Responsible Entities can have a single LEAP that controls the LERC from more than one BES asset containing low impact BES Cyber Systems. However the LERC between assets "behind" the LEAP and another asset containing a low impact BES Cyber System must also pass through the single LEAP. Locating the LEAP at an external location with multiple BES assets containing low impact BES Cyber Systems "behind" it should not allow unfettered access from one BES asset to all other BES assets sharing the LEAP. It is also not the intent of the SDT where low impact BES Cyber Systems do not have any LERC that additional connectivity be established nor that a LEAP be established.

The electronic access controls should address the risk of using the asset's LERC or Dial-up Connectivity~~external connectivity~~ to gain access to the low impact BES Cyber Systems. For LERC, a LEAP shall be implemented that permits only necessary inbound and outbound access and denies all other access.~~The entity should be able to describe how its electronic access controls on the external connectivity paths protect the collection of low impact BES Cyber Systems at the site. The intent is to reduce the risk of aggregation of numerous low impact BES Cyber Systems at the site or across multiple sites through external connectivity.~~

Examples of sufficient access controls may include:

- ~~All the external routable protocol connectivity paths to~~Any LERC for the asset passes through a ~~firewall~~ LEAP that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are ~~shielded from or to the world wide web~~confined to only those that the Responsible Entity deems necessary (e.g. IP addresses, ports, services~~, and/or data diode~~) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.
- Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no autoanswer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely

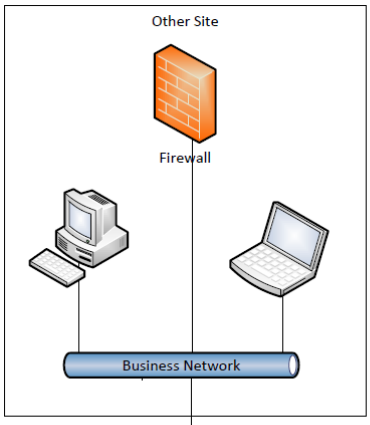
controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has ~~dialup~~ Dial-up ~~connectivity~~ Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset ~~which~~ that has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

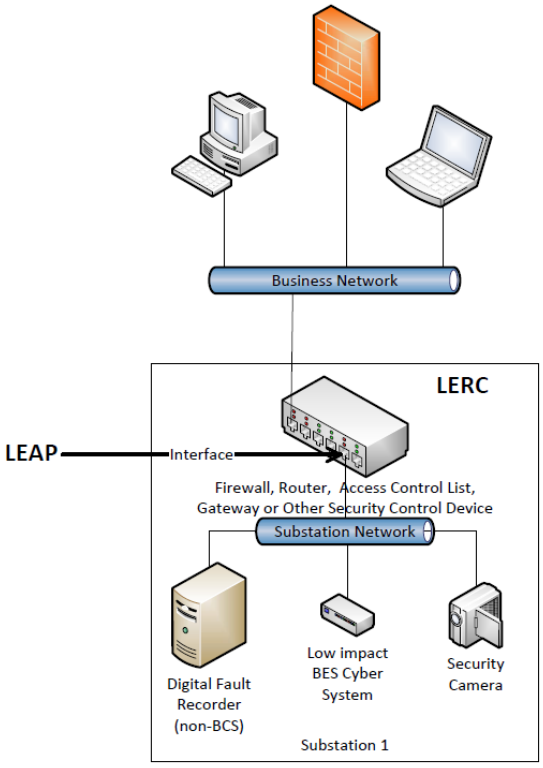
The SDT also notes ~~that in topic 2.4, the SDT~~it uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

The following diagrams explain the SDT's rationale.



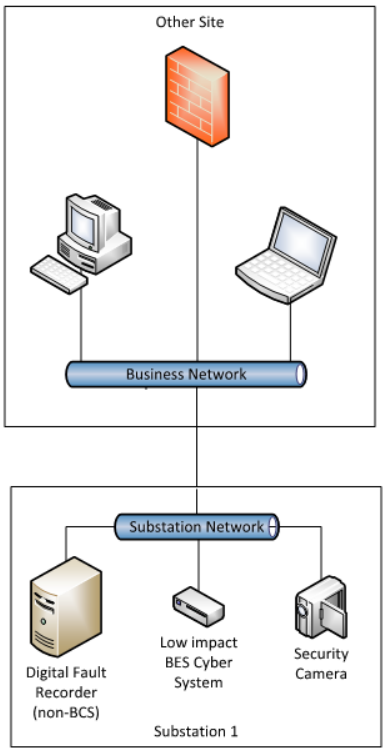
REFERENCE MODEL - 1

The low impact BES Cyber System is behind a LEAP. In this example, the LEAP is the network interface on the low impact BES Cyber System. The host-based firewall restricts electronic access for Low Impact External Routable Connectivity (LERC).



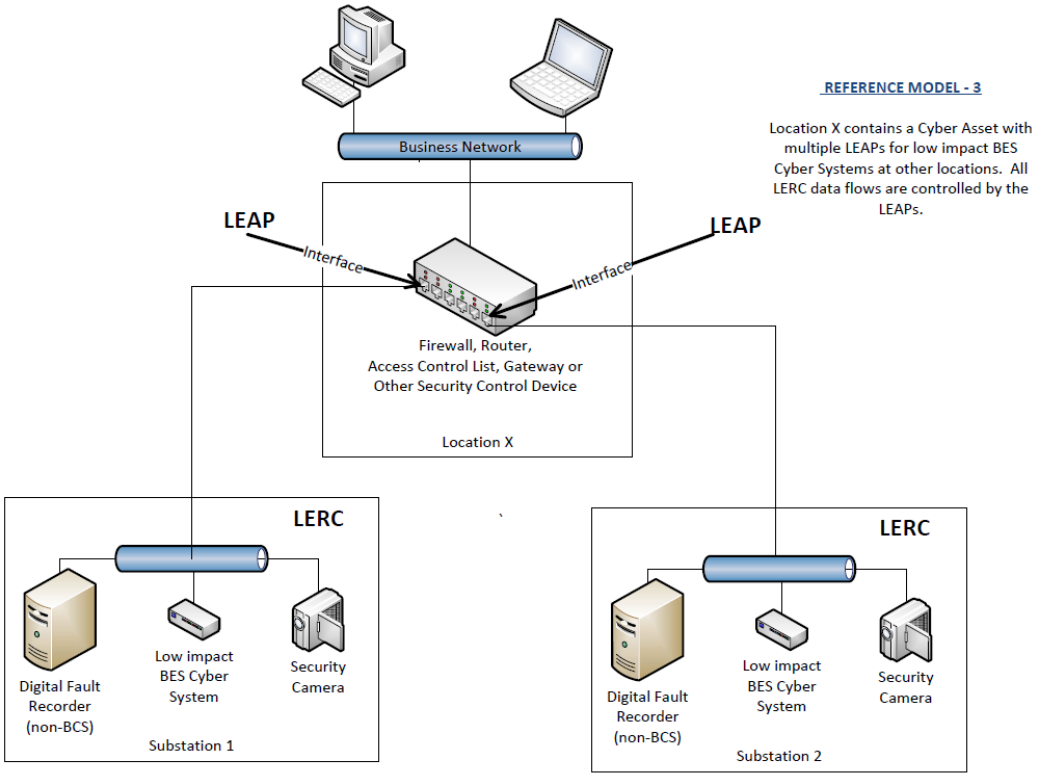
REFERENCE MODEL - 2

All LERC to the low impact BES Cyber System is controlled by an LEAP.



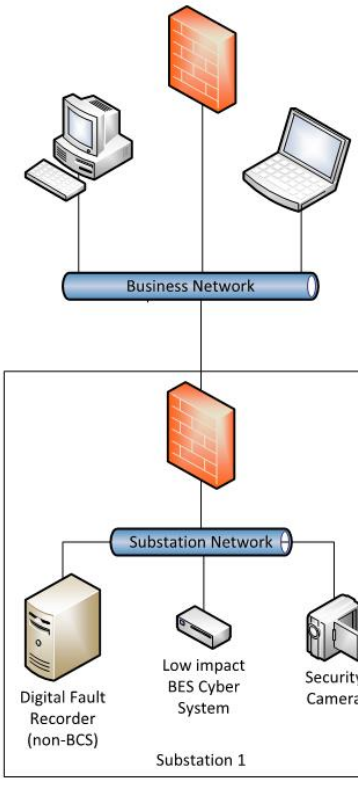
NOT OK

The BES Cyber System is behind an access point, however all external routable protocol paths to the BES Cyber System are not controlled by an access point if they originate on the business network.



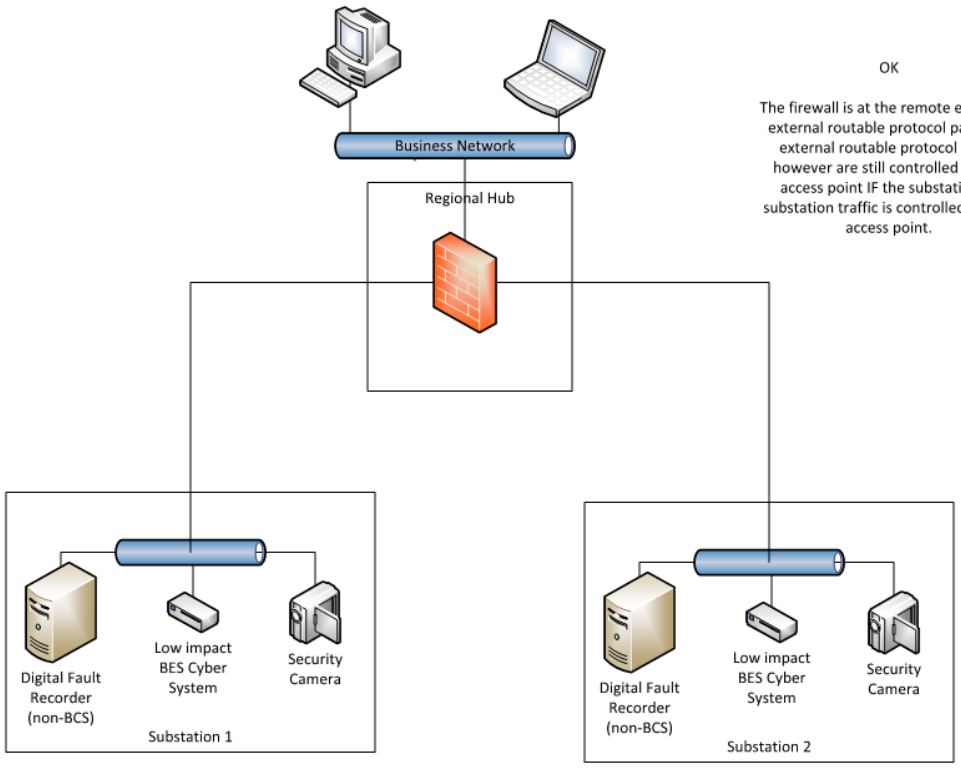
REFERENCE MODEL - 3

Location X contains a Cyber Asset with multiple LEAPs for low impact BES Cyber Systems at other locations. All LERC data flows are controlled by the LEAPs.



OK

All the external traffic to the BES Cyber System is controlled by an access point.



Requirement R2 Attachment 1 – Cyber Security Incident Response~~2.5 –~~

The entity should have ~~a~~ one or more documented cyber security incident response plans that include~~s~~ each of the topics listed. For assets that do not have LERC~~have limited or no connectivity~~, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or ~~paper~~ drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed. It is the intent of the SDT to have the cyber security incident response plan(s) kept current which includes updating the plan(s) within 180 days following a test or an actual incident.

In the event of a Reportable Cyber Security Incident, Attachment 1, element 4.6 specifies entities must retain relevant records for Reportable Cyber Security Incidents. Example evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-

incident review notes. Entities should refer to their handling procedures to determine the types of evidence to retain. The evidence retention period for records related to Reportable Cyber Security Incidents is defined in Section C.1.2 of this Standard, which is the same for all requirements in CIP-003-6.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

~~2.6 - The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel on at least a quarterly basis. The physical security, electronic access controls, and the cyber security incident response plan should be covered at least every 15 months. It is up to the entity as to the topics and how it schedules these topics. It should be sufficient for an entity to produce the awareness material that it delivered quarterly and the delivery method(s) (posters, emails, topics at staff meetings, etc.). The intent is that tracking of reception of the messages by personnel is not required.~~**Requirement R3:**

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation

Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014

Description of Current Draft

This draft standard is being posted for an additional comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 4. EACMS; 5. PACS; and 6. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: **1.** EACMS; and **2.** PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with tools used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, the Requirement R4 is a new requirement developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1, except under CIP Exceptional Circumstances. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable elements in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per element are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document the Removable Media elements according to CIP-010-2, Requirement R4, Attachment 1, element 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, element 1.1. (R4)	implement the Removable Media elements according to CIP-010-2, Requirement R4, Attachment 1, element 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement R4,	implement mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, elements 1.2, 1.3, and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of security	Removable Media according to CIP-010-2, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, elements 1.2, 1.3, and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by Vendors or Contractors according to CIP-010-2, Requirement R4, Attachment 1, elements 2.1 and 2.2. (R4)	vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by Vendors or Contractors according to CIP-010-2, Requirement R4, Attachment 1, elements 2.1 and 2.2. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-010-2 - Attachment 1

Required Elements for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the elements provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

1. Transient Cyber Asset(s) Owned or Managed by the Responsible Entity.

1.1. Transient Cyber Asset management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall specify:

1.2.1. Authorized users, either individually or by group or role;

1.2.2. Authorized locations, either individually or by group; and

1.2.3. Authorized uses, which shall be limited to what is necessary to perform business functions.

1.3. Security vulnerability mitigation: To mitigate security vulnerabilities (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate security vulnerabilities.

1.4. Introduction of malicious code mitigation: To mitigate the introduction of malicious code (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Risk of unauthorized use mitigation: To mitigate the risk of unauthorized use, each Responsible Entity shall use one or a combination of the following methods:

- Transient Cyber Asset resides within a location with restricted physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication;
- Theft recovery tools; or
- Other method(s) to mitigate the risk of unauthorized use.

2. Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors.

2.1 Security vulnerability mitigation: To mitigate security vulnerabilities (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Review of installed security patch(es);
- Review of security patching process used by the vendor or contractor;
- Review of other vulnerability mitigation performed by the vendor or contractor; or
- Other method(s) to mitigate security vulnerabilities.

2.2 Malicious code mitigation: To mitigate malicious code, each Responsible Entity shall use one or a combination of the following methods:

- Review of antivirus update level;
- Review of antivirus update process used by the vendor or contractor;
- Review of application whitelisting used by the vendor or contractor;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the vendor or contractor; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate security vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the vendor- or contractor-owned Transient Cyber Asset.

3. Removable Media

3.1. Removable Media authorization: For each individual or group of Removable Media, each Responsible Entity shall specify:

3.1.1. Authorized users, either individually or by group or role; and

3.1.2. Authorized locations, either individually or by group.

3.2. Malicious code mitigation: To mitigate malicious code, each Responsible Entity shall scan Removable Media outside of the BES Cyber System.

CIP-010-2 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Element 1.1: Examples of evidence for element 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) Owned or Managed by the Responsible Entity or part of a security policy.

Element 1.2: Examples of evidence for element 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Transient Cyber Asset(s) Owned or Managed by the Responsible Entity. The documentation must identify the Transient Cyber Asset, individually or by group of Transient Cyber Asset(s) along with the authorized users, either individually or by group or role, the authorized locations, either individually or by group and the authorized uses associated with what is necessary to perform business functions.

Element 1.3: Examples of evidence for element 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate security vulnerabilities such as security patch management implementation, the use of live operating systems, system hardening practices or other method(s) to mitigate security vulnerability. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 1.4: Examples of evidence for element 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 1.5: Examples of evidence for element 1.5 may include, but are not limited to documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; method(s) of the theft recovery tools; or documentation of other method(s) to mitigate the risk of unauthorized use. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.1: Examples of evidence for element 2.1 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memorandums, electronic mail, policies or contracts from vendors or contractors that identify the security patching process or vulnerability mitigation performed by the vendor or contractor; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate security vulnerabilities for Transient Cyber Asset(s) Owned of Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.2: Examples of evidence for element 2.2 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed the antivirus update level; memorandums, electronic mail, system documentation, policies or contracts from vendors or contractors that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the vendor or contractor; evidence from change management systems, electronic mail or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.3: Examples of evidence for element 2.3 may include, but are not limited to documentation from change management systems, electronic mail, contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the vendor or contractor owned Transient Cyber Asset.

Element 3.1: Examples of evidence for element 3.1 may include, but are not limited to documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role and the authorized locations, either individually or by group.

Element 3.2: Examples of evidence for element 3.2 may include, but are not limited to documentation of the method(s) used to mitigate malicious code such as results of scans of the media, or documented confirmation by the entity that the media was deemed to be free of malicious code. Confirmation can be documented through email or within change management record(s).

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks. Because of this, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas that are needed to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. These assets do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment
- Packet sniffers
- Equipment used for BES Cyber System maintenance

- Equipment used for BES Cyber System configuration
- Equipment used to perform vulnerability assessments

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, element 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and applications of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management. These are broken down as follows:

1. Transient Cyber Asset(s) Owned or Managed by the Responsible Entity
2. Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors
3. Removable Media

<u>Per Transient Cyber Asset Capability</u>

As with other CIP standards, the requirements are intended for an entity to perform the security functions that the system is capable of doing. The use of this phrase is to eliminate the need for a technical feasibility exception when it is understood that the device cannot perform a function. Using the example of malicious code, many types of appliances are not capable of implementing antivirus software and therefore the software would not be required since it is not a capability of the device.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option that is most appropriate. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the device.

Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by the Responsible Entity

Element 1.1: Entities have a high level of control for the assets that they own or manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods.

Element 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct ownership or management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks, and approved network interfaces (e.g. wireless including near field communication or Bluetooth and wires connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g. wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Element 1.3: Entities are to document and implement their process(es) to mitigate security vulnerabilities through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in security vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how their Transient Cyber Asset(s) will be used. It is possible for an entity to have their Transient Cyber Asset be part of an enterprise

patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike, CIP-007, R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.

- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating customer live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate security vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet security vulnerability mitigation.

Element 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns provides flexibility just as with security patching, to manage their Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, it is possible that entities can choose for devices that do not regularly connect to receive scheduled updates, to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate from the Transient Cyber Asset to the BES Cyber Asset of BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial

or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.

- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the introduction of malicious code.

Element 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks of unauthorized use to the Transient Cyber Asset.

- Transient Cyber Asset resides within a location with restricted physical access. The intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location that manages unauthorized physical access to the device.
- Full disk encryption with authentication is an option that can be used to protect a Transient Cyber Asset from unauthorized physical access. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents anything being read from the hard disk until the user has confirmed they have the correct password or other credentials.
- Multi-factor authentication is used to ensure the identity of the person accessing the device.
- Theft recovery tools that can be used to remotely wipe or lockout systems if they are stolen or lost.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of unauthorized use.

Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors

The attachment also recognizes the lack of control for Transient Cyber Assets that are owned or managed by vendors or contractors. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with vendors and contractors to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department Of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Elements from the procurement language may unify vendor and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP Program elements may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the vendor's support. Entities should consider the elements of the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Element 2.1: Entities are to document and implement their process(es) to mitigate security vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the vendor or contractor managed Transient Cyber Asset to determine whether the security patch level of the device is adequate to mitigate the risk of security vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the vendor or contractor security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of security vulnerabilities to applicable systems.
- Conduct a review of other processes that the vendor or contactor uses to mitigate the risk of security vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate security vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of security vulnerabilities

Element 2.2: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the vendor or contactor to ensure that their processes are adequate to the Responsible Entity to reduce the risk of introducing malicious software to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of application whitelisting used by the vendor or contractor to reduce the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the vendor or contractor to ensure that unnecessary ports, services, applications, etc have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Element 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the vendor or contractor owned Transient Cyber Asset. The intent of this element is to ensure that after conducting the selected review from elements 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entities security posture, the vendor or contractor is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement 4 Attachment 1 Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Element 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Element 3.2: Entities are to document and implement their process(es) to mitigate malicious code through the use of scanning the Removable Media before it is connected to a BES Cyber Asset. The scanning is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014

Description of Current Draft

This draft standard is being posted for an ~~initial~~ additional comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
~~First 45-Day Comment Period Opens~~	~~June 2014~~
Additional 45-Day Comment Period ~~(if necessary)~~	~~August~~ September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-2

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 4. EACMS; 5. PACS; and 6. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: **1.** EACMS; and **2.** PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 ~~is to address~~responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, ~~which require the standards~~ to address security-related issues associated with tools ~~specifically~~ used on a temporary basis for tasks such as~~for~~ data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To ~~that end~~mitigate the risks associated with such tools, the R~~r~~equirement R4 ~~goals are as follows~~is a new requirement developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

~~The SDT has incorporated~~Requirement R4 incorporates the concepts ~~of~~from other CIP requirements ~~from FERC-approved~~in CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. ~~While the requirements are similar, they are not to the same rigor of those found in CIP-007 protecting the permanent assets identified by an entity.~~ A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more documented ~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media* Protection~~ plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1, except under CIP Exceptional Circumstances. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable elements in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per element are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or

Removable MediaEvidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. Authorization shall include: 4.1.1. Users, individually or by group/role; 4.1.2. Locations, individually or by group/role; 4.1.3. Defined acceptable use; and 4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or • A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.

~~CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~4.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~• PCA~~	~~Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).~~
~~4.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~• PCA~~	~~Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).~~
~~4.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~• PCA~~	~~Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• Records of response processes for malicious code detection~~ ~~• Records of the performance of these processes when malicious code is detected.~~
~~4.5~~	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~• PCA~~	~~Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.~~	~~An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.~~

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	Applicable Systems	Requirements	Measures
4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4. For a modification that deviates from the state in Part 4.1.4, either: • Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or • Update Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.
4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date. For security patches that are not up-to-date, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance ~~Violation~~ Investigations

Self-Reporting

Complaints ~~Text~~

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document the Removable Media elements according to CIP-010-2, Requirement R4, Attachment 1, element 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, element 1.1. (R4) ~~The Responsible~~	implement the Removable Media elements according to CIP-010-2, Requirement R4, Attachment 1, element 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement	implement mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, elements 1.2, 1.3, and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of security vulnerabilities or mitigation for the	Removable Media according to CIP-010-2, Requirement R4. (R4) ~~The Responsible Entity did not document or implement process(es) that collectively address the requirement parts as required by Requirement R4. (R4)~~ ~~OR~~ ~~The Responsible Entity did not use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability) as required by Requirement R4, Part 4.2. (4.2)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Entity has documented and implemented process(es) addressing authorization of use of Transient Cyber Assets, but failed to include one of the required items listed in 4.1.1 through 4.1.4. (4.1)~~	R4, Attachment 1, elements 1.2, 1.3, and 1.4. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of security vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets Owned or Managed by Vendors or Contractors according to CIP-010-2, Requirement R4, Attachment 1, elements 2.1 and	introduction of malicious code for Transient Cyber Assets Owned or Managed by Vendors or Contractors according to CIP-010-2, Requirement R4, Attachment 1, elements 2.1 and 2.2. (R4) ~~The Responsible Entity has documented and implemented process(es) addressing authorization of use of Transient Cyber Assets, but failed to include three of the required items listed in 4.1.1 through 4.1.4. (4.1)~~ ~~OR~~ ~~The Responsible~~	~~The Responsible Entity did not use method(s) to detect malicious code on Removable Media prior to use on applicable systems as required by Requirement R4, Part 4.3. (4.3)~~ ~~OR~~ ~~The Responsible Entity did not mitigate the threat of detected malicious code for Transient Cyber Assets or Removable Media as required by Requirement R4, Part 4.4. (4.4)~~ ~~OR~~ ~~The Responsible Entity did not update signatures or patterns for those methods~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				2.2. (R4) ~~The Responsible Entity has documented and implemented process(es) addressing authorization of use of Transient Cyber Assets, but failed to include two of the required items listed in 4.1.1 through 4.1.4. (4.1)~~	~~Entity documented and implemented a process to evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 but did not take one of the actions required by Requirement R4, Part 4.6. (4.6)~~ ~~OR~~ ~~The Responsible Entity documented and implemented a process to evaluate Transient Cyber Assets within 35 calendar days prior to use but did not take one of the actions required by Requirement R4, Part 4.7. (4.7)~~	~~identified in Parts 4.2 and 4.3 that use signatures or patterns as required by Requirement R4, Part 4.5. (4.5)~~ ~~OR~~ ~~The Responsible Entity did not evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 as required by Requirement R4, Part 4.6. (4.6)~~ ~~OR~~ ~~The Responsible Entity did not evaluate Transient Cyber Assets within 35 calendar days prior to use as required by Requirement R4, Part~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~4.7. (4.7)~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-010-2 - Attachment 1

Required Elements for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the elements provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

1. Transient Cyber Asset(s) Owned or Managed by the Responsible Entity.

1.1. Transient Cyber Asset management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall specify:

1.2.1. Authorized users, either individually or by group or role;

1.2.2. Authorized locations, either individually or by group; and

1.2.3. Authorized uses, which shall be limited to what is necessary to perform business functions.

1.3. Security vulnerability mitigation: To mitigate security vulnerabilities (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate security vulnerabilities.

1.4. Introduction of malicious code mitigation: To mitigate the introduction of malicious code (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Risk of unauthorized use mitigation: To mitigate the risk of unauthorized use, each Responsible Entity shall use one or a combination of the following methods:

- Transient Cyber Asset resides within a location with restricted physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication;
- Theft recovery tools; or
- Other method(s) to mitigate the risk of unauthorized use.

2. Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors.

2.1 Security vulnerability mitigation: To mitigate security vulnerabilities (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Review of installed security patch(es);
- Review of security patching process used by the vendor or contractor;
- Review of other vulnerability mitigation performed by the vendor or contractor; or
- Other method(s) to mitigate security vulnerabilities.

2.2 Malicious code mitigation: To mitigate malicious code, each Responsible Entity shall use one or a combination of the following methods:

- Review of antivirus update level;
- Review of antivirus update process used by the vendor or contractor;
- Review of application whitelisting used by the vendor or contractor;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the vendor or contractor; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate security vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the vendor- or contractor-owned Transient Cyber Asset.

3. Removable Media

3.1. Removable Media authorization: For each individual or group of Removable Media, each Responsible Entity shall specify:

3.1.1. Authorized users, either individually or by group or role; and

3.1.2. Authorized locations, either individually or by group.

3.2. Malicious code mitigation: To mitigate malicious code, each Responsible Entity shall scan Removable Media outside of the BES Cyber System.

CIP-010-2 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Element 1.1: Examples of evidence for element 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) Owned or Managed by the Responsible Entity or part of a security policy.

Element 1.2: Examples of evidence for element 1.2 may include, but are not limited to,~~:~~ documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Transient Cyber Asset(s) Owned or Managed by the Responsible Entity. The documentation must identify the Transient Cyber Asset, individually or by group of Transient Cyber Asset(s) along with the authorized users, either individually or by group or role, the authorized locations, either individually or by group and the authorized uses associated with what is necessary to perform business functions.

Element 1.3: Examples of evidence for element 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate security vulnerabilities such as security patch management implementation, the use of live operating systems, system hardening practices or other method(s) to mitigate security vulnerability. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 1.4: Examples of evidence for element 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 1.5: Examples of evidence for element 1.5 may include, but are not limited to documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; method(s) of the theft recovery tools; or documentation of other method(s) to mitigate the risk of unauthorized use. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.1: Examples of evidence for element 2.1 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memorandums, electronic mail, policies or contracts from vendors or contractors that identify the security patching process or vulnerability mitigation performed by the vendor or contractor; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate security vulnerabilities for Transient Cyber Asset(s) Owned of Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.2: Examples of evidence for element 2.2 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed the antivirus update level; memorandums, electronic mail, system documentation, policies or contracts from vendors or contractors that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the vendor or contractor; evidence from change management systems, electronic mail or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.3: Examples of evidence for element 2.3 may include, but are not limited to documentation from change management systems, electronic mail, contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the vendor or contractor owned Transient Cyber Asset.

Element 3.1: Examples of evidence for element 3.1 may include, but are not limited to documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role and the authorized locations, either individually or by group.

Element 3.2: Examples of evidence for element 3.2 may include, but are not limited to documentation of the method(s) used to mitigate malicious code such as results of scans of the media, or documented confirmation by the entity that the media was deemed to be free of malicious code. Confirmation can be documented through email or within change management record(s).

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks. Because of this, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas that are needed to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. These assets do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

~~This Requirement applies to any transient devices (i.e. Transient Cyber Assets and Removable Media) that will be connected temporarily to an applicable system. Examples of these devices include, but are not limited to:~~

- ~~Hardware/software~~ Ddiagnostic test equipment

- ~~Hardware/software P~~packet sniffers
- ~~Hardware/software~~Equipment used for BES Cyber System maintenance
- ~~Hardware/software~~Equipment used for BES Cyber System configuration
- ~~Hardware/software~~Equipment used to perform vulnerability assessments

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, element 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and applications of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management. These are broken down as follows:

1. Transient Cyber Asset(s) Owned or Managed by the Responsible Entity
2. Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors
3. Removable Media

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to perform the security functions that the system is capable of doing. The use of this phrase is to eliminate the need for a technical feasibility exception when it is understood that the device cannot perform a function. Using the example of malicious code, many types of appliances are not capable of implementing antivirus software and therefore the software would not be required since it is not a capability of the device.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option that is most appropriate. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the device.

Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by the Responsible Entity

Element 1.1: Entities have a high level of control for the assets that they own or manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods.

Element 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct ownership or management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks, and approved network interfaces (e.g. wireless including near field communication or Bluetooth and wires connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

~~Transient Cyber Assets can be in the form of a laptop, desktop, or tablet. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~This requirement does not cover hardware/software components that may support information system maintenance yet are a part of the system, for example the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of a switch.~~

~~Requirement Parts 4.1, 4.3, 4.6, and 4.7 refer to the term "prior to use" related to when specific actions must occur. For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. For example, a technician would need to have a laptop evaluated only once according to Part 4.6 when working in the same PSP. The technician would not need to have the evaluation performed each time it connects to a different Cyber Asset.~~

~~**Requirement Part 4.1:**~~

~~Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets. This allows entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection. The Transient Cyber Assets~~

~~may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:~~

~~**1.** User(s), individually or by group/role, allowed to use Transient Cyber Assets. This is intended to provide assurance around who has physical proximity to the Transient Cyber Assets. These user(s) must have authorized electronic and unescorted physical access to the applicable system in accordance with CIP-004.~~

~~**2.** Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group/role of locations. Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. It may be reasonable to have separate Transient Cyber Assets for each impact level.~~

~~**3.** The intended or approved use of each Transient Cyber Asset. Activities not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals on the activities or uses that are not allowed (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).~~

~~**4.** The operating system, firmware, and intentionally installed software. All of this information may not be available or relevant to each Transient Cyber Asset. Having this information facilitates the review in Part 4.6. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The Standard Drafting Team does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included.~~

~~CAUTION:~~ Entities should exercise caution when using Transient Cyber Assets and ensure they do not have ~~wireless or Bluetooth~~ features enabled (e.g. wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Element 1.3: Entities are to document and implement their process(es) to mitigate security vulnerabilities through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in

security vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how their Transient Cyber Asset(s) will be used. It is possible for an entity to have their Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike, CIP-007, R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating customer live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate security vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet security vulnerability mitigation.

Element 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns provides flexibility just as with security patching, to manage their Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, it is possible that entities can choose for devices that do not regularly connect to receive scheduled updates, to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate from the Transient Cyber Asset to the BES Cyber Asset of BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the introduction of malicious code.

Element 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks of unauthorized use to the Transient Cyber Asset.

- Transient Cyber Asset resides within a location with restricted physical access. The intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location that manages unauthorized physical access to the device.
- Full disk encryption with authentication is an option that can be used to protect a Transient Cyber Asset from unauthorized physical access. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents anything being read from the hard disk until the user has confirmed they have the correct password or other credentials.
- Multi-factor authentication is used to ensure the identity of the person accessing the device.
- Theft recovery tools that can be used to remotely wipe or lockout systems if they are stolen or lost.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of unauthorized use.

~~**Requirement Parts 4.2, 4.3, 4.4, and 4.5:**~~

~~Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.~~

~~It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.~~

~~For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.~~

~~For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.~~

~~Requirement Parts 4.6 and 4.7:~~

~~Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.~~

~~Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.~~

~~Requirement Parts 4.2, 4.3, 4.4, and 4.5:~~

~~Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of~~

~~connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.~~

~~It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.~~

~~For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.~~

~~For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.~~

~~Requirement Parts 4.6 and 4.7:~~

~~Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.~~

~~Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.~~

Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors

The attachment also recognizes the lack of control for Transient Cyber Assets that are owned or managed by vendors or contractors. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with vendors and contractors to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department Of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Elements from the procurement language may unify vendor and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP Program elements may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the vendor's support. Entities should consider the elements of the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Element 2.1: Entities are to document and implement their process(es) to mitigate security vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the vendor or contractor managed Transient Cyber Asset to determine whether the security patch level of the device is adequate to mitigate the risk of security vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the vendor or contractor security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of security vulnerabilities to applicable systems.
- Conduct a review of other processes that the vendor or contactor uses to mitigate the risk of security vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate security vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of security vulnerabilities

Element 2.2: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the vendor or contactor to ensure that their processes are adequate to the Responsible Entity to reduce the risk of introducing malicious software to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of application whitelisting used by the vendor or contractor to reduce the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the vendor or contractor to ensure that unnecessary ports, services, applications, etc have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Element 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the vendor or contractor owned Transient Cyber Asset. The intent of this element is to ensure that after conducting the selected review from elements 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entities security posture, the vendor or contractor is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement 4 Attachment 1 Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Element 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Element 3.2: Entities are to document and implement their process(es) to mitigate malicious code through the use of scanning the Removable Media before it is connected to a BES Cyber Asset. The scanning is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-003.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-X

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-X, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-X.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These

delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 18 calendar months of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 15 calendar months but did complete this review	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 16 calendar months but did	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2)	The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R4)	calendar days but did document this change in less than 50 calendar days of the change. (R4)	calendar days of the change. (R4)	from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-X, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-X, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-X, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-X, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-X, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-X, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-X, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. ~~2.~~ First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional ~~initial~~ comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the ~~directives of~~ FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-003.

Anticipated Actions	Anticipated Date
~~First 45-Day Comment Period Opens~~	~~June 2014~~
Additional 45-Day Comment Period ~~(if necessary)~~	~~August~~ September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~5~~X

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~5~~X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-X, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-X.

6. Background:

Standard CIP-003~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which ~~-CIP-002-5.1~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~-CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies, . . .~~**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes,

but ~~they~~ it must address the applicable requirements. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to ~~its~~ low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only three~~one of the topics as required by Requirement R2 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R2) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for assets with a low~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only~~ two of the topics as required by Requirement R2 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R2) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only one~~three of the topics as required by Requirement R2 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R2) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2~~	The Responsible Entity did not ~~document or implement~~have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR	~~assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2)	~~but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the	within 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	CIP Senior Manager ~~according to Requirement R2~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior	The Responsible Entity has identified by name a CIP Senior	The Responsible Entity has identified by name a CIP Senior Manager, but	The Responsible Entity has not identified, by name,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than	~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4)~~	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			40 calendar days of the change. (R4)	50 calendar days of the change. (R4)	~~OR~~ ~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4)~~ ~~OR~~ The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-~~5~~X, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~5~~X, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-~~5~~X, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-~~5~~X, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~5~~X, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems

is not necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-~~5~~X, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~5~~X, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-004.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-X

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-X:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-004-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-X Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-X Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for

CIP-004-X Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-X Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-X Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-X Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-X Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-X. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-X and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-X Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-X Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity	did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			(3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR The Responsible Entity has implemented	individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last

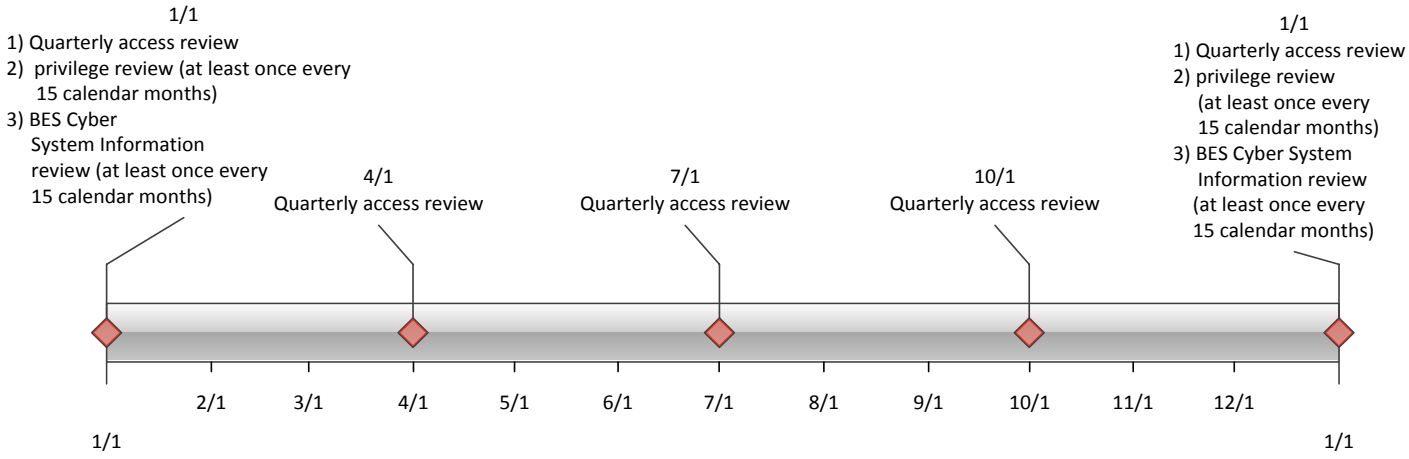
PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the

individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. ~~2.~~ First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional~~initial~~ comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet ~~the directives of~~ FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-004.

Anticipated Actions	Anticipated Date
~~First 45-Day Comment Period Opens~~	~~June 2014~~
Additional 45-Day Comment Period ~~(if necessary)~~	~~August~~ September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~5.1~~X

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~5.1~~X:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-004-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-004~~-5.1~~ exists as part of a suite of CIP Standards related to cyber security, which~~.~~ ~~CIP-002-5~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards.*~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements~~

~~described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~X Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for

CIP-004-~~5.1~~X Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ ~~a~~ one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~5.1~~X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~5.1~~X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~5.1~~X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~5.1~~X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-~~5~~X. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-~~5~~ X and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R4 – Access Management Program. [Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~5.1~~X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~5.1~~X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~5.1~~X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-~~5.1~~X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~X Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~5.1~~X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~5.1~~X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-~~5.1~~X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~5.1~~ X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the~~	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the~~	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	~~deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical	~~deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	(2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date~~, and did not identify, assess and correct the deficiencies~~. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals~~, and did not identify, assess, and correct the deficiencies~~.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals~~, and did not identify, assess, and correct the deficiencies~~.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date ~~and has identified deficiencies, and did not identify, assess, and correct the deficiencies~~. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)			
R4	**Operations Planning and Same Day Operations**	~~Lower~~Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter~~, and did not identify, assess and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located~~, and did not identify, assess, and correct the deficiencies~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.4)			were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that- an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that -an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that -an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances~~, and did not~~			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5~~ 1X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~identify, assess, and correct the deficiencies~~. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last

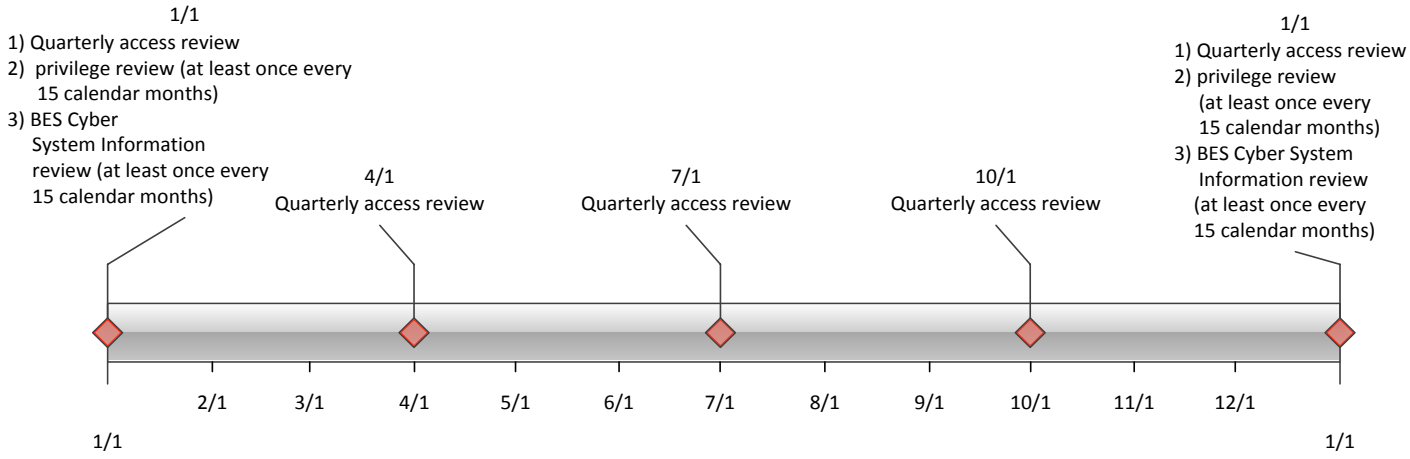
PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the

individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-007.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-X

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-007-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-X, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-X.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-X Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-X Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3)es.	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R3. (R3)ies. OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-X Table R5*. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch

management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity

levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they

may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period

called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common

configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password

guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional ~~initial~~ comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the ~~directives of~~ FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-007.

Anticipated Actions	Anticipated Date
~~First 45-Day Comment Period Opens~~	~~June 2014~~
Additional 45-Day Comment Period ~~(if necessary)~~	~~August~~ September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-~~6~~X

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~6~~X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-007-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-X, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-X.

6. Background:

Standard CIP-007 ~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5.1~~ requires the initial identification and categorization of BES Cyber Systems~~. CIP-003-5~~6, ~~CIP-004-5~~6, ~~CIP-005-5, CIP-006-5~~6, ~~CIP-007-5~~6, ~~CIP-008-5, CIP-009-5~~6, ~~CIP-010-1~~2, ~~and CIP-011-1~~ 2~~-~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on~~

~~*whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is

specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~6~~ X Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~6~~ X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring

minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**

5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.2) ~~OR~~ ~~The Responsible Entity has~~	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.1) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for determining~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R1) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)~~	~~necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)~~	~~the deficiencies. (R1)~~
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R2 ~~and has identified deficiencies but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but~~	sources, for tracking or evaluating cyber security patches for applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or~~	applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and	~~not assess or correct the deficiencies~~. (R2)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2)~~ OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35	~~correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2)	implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for~~	security patches for applicable Cyber Assets~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but less than 50 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation~~	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct~~	~~applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4)~~OR~~ ~~The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess,~~	plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an~~	~~not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4)~~ OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4) ~~OR~~ ~~The Responsible Entity documented~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~or correct the deficiencies. (2.3)~~	~~existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)~~
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns ~~and has identified deficiencies but did~~	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code ~~and has identified deficiencies but did not assess or correct~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R3 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R3) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~not assess or correct the deficiencies~~. (3.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)~~	~~the deficiencies~~. (3.2)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used,	~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify, assess, or correct the deficiencies. (R3)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code~~ and has identified deficiencies but did not assess or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the Responsible Entity did not update malicious code protections ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (3.3)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies.~~ ~~(3.3)~~	~~the deficiencies~~. (3.1) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies.~~ ~~(3.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4) ~~The Responsible Entity has documented and~~	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.2)~~OR~~ ~~The Responsible Entity has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R4 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R4)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4~~	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2)~~ OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.1) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log events for the~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.3) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional~~	~~Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3)~~OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals~~ and has identified deficiencies but did~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (4.4)~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)~~	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for~~	process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~The Responsible Entity has implemented one or more documented process(es) for password-only~~	process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the~~	more process(es) that included the applicable items in *CIP-007-~~6~~ X Table R5 ~~and has identified deficiencies but did not assess or correct the deficiencies~~*. (R5) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5)~~OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2)~~OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts~~ and has identified deficiencies but did~~	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (5.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only	authentication of interactive user access~~ and did not identify, assess, or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.4) ~~OR~~ ~~The Responsible Entity has~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce	~~implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					one of the two password parameters as described in 5.5.1 and 5.5.2 ~~and did not identify, assess, or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months	described in 5.5.1 and 5.5.2 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password~~	~~or correct the deficiencies. (5.5)~~ OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.7)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~6~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)~~

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch

management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity

levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, ~~portable storage media policies,~~ Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are

of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period

called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common

configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password

guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-010.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-X

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-X Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-X Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-X Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-X Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-X Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-X Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-X Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-X Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-X Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-X Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. ~~2.~~ First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional ~~initial~~ comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the ~~directives of~~ FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-010.

Anticipated Actions	Anticipated Date
~~First 45-Day Comment Period Opens~~	~~June 2014~~
Additional 45-Day Comment Period ~~(if necessary)~~	~~August~~ September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-~~1~~X

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-~~1~~X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-010 ~~-1~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability

standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ X Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ X Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~1~~ X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~1~~ X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~1~~ X Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ X Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ X Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ X Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ X Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ X Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ X Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~1~~ X Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~1~~ X Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified~~	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible~~	~~identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required~~	~~deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for~~	~~implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct~~	~~security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1)~~	~~changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update~~	update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~the deficiencies in the verification documentation. (1.4.3)~~		~~baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the~~	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in~~	configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencie~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~(1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~identified deficiencies but did not assess or correct the deficiencies. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)~~OR~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~not identify, assess, or correct the deficiencies. (2.1)~~
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-~~5~~6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-~~5~~ 6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-011.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-X

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-011-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-011exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-X Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity

must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. ~~2.~~ First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

Description of Current Draft

This draft standard is being posted for an additional ~~initial~~ comment and ballot to ballot the removal of "identify, assess, and correct" language. The draft includes modifications to meet the ~~directives of~~ FERC Order No. 791 directive to remove or modify the "identify, assess, and correct" language from CIP-011.

Anticipated Actions	Anticipated Date
~~First 45-Day Comment Period Opens~~	~~June 2014~~
Additional 45-Day Comment Period ~~(if necessary)~~	~~August~~ September 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
X	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~1~~X

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~1~~X:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-011-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-011 ~~-1~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it~~-~~ believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~1~~ X Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~1~~ X -Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ X Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~1~~ X Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~1~~ X Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~1~~ X Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-~~1~~ X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify,~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~assess, or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~but did not identify, assess, or correct the deficiencies. (1.2)~~	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity

must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Definitions of Terms Used in Standards

This section includes all newly defined or revised terms used in the proposed standards. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that allows Low Impact External Routable Connectivity. The Cyber Asset may reside at a location external to the asset or assets containing low impact BES Cyber Systems. The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System.

Low Impact External Routable Connectivity (LERC): Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s). Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Definitions of Terms Used in Standards

This section includes all newly defined or revised terms used in the proposed standards. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

Removable Media: Media, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, or access data. Removable Media are not Cyber Assets. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset: A Cyber Asset, (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Definitions of Terms Used in Standards

This section includes all newly defined or revised terms used in the proposed standards. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standards are approved. When the standards become effective, these defined terms will be added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. ~~A Transient Cyber Asset is not a BES Cyber Asset.~~

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. ~~A Transient Cyber Asset is not a Protected Cyber Asset.~~

Removable Media: ~~Portable media~~Media, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, ~~and/~~or access data. Removable Media are not Cyber Assets. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. ~~A Cyber Asset is not Removable Media.~~

Transient Cyber Asset: A Cyber Asset, (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

September 3, 2014

Requested Approvals

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel and Training
- CIP-006-6 — Cyber Security — Physical Security
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009–6 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-2 — Cyber Security — Configuration Change Management
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5 — Cyber Security — Personnel and Training
- CIP-006-5 — Cyber Security — Physical Security
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	Media, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, or access data. Removable Media are not Cyber Assets. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Transient Cyber Asset	A Cyber Asset, directly connected (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not

	limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Low Impact BES Cyber System Electronic Access Point (LEAP)	A Cyber Asset interface that allows Low Impact External Routable Connectivity. The Cyber Asset may reside at a location external to the asset or assets containing low impact BES Cyber Systems. The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System.
Low Impact External Routable Connectivity (LERC)	Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s). Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date that entities must begin to comply that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. <u>CIP-003-6 — Cyber Security — Security Management Controls</u>

   Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the

first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-003-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Requirement R2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 1

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 3

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 4

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

2. CIP-004-6 — Cyber Security — Personnel and Training

   Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security

   Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-006-6, Requirement R1, Part 1.10

   For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-6 —Cyber Security — Systems Security Management

   Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable

governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems

Reliability Standard CIP–009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-2 — Cyber Security — Configuration Change Management

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-010-2, Requirement R4

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

7. CIP-011-2 — Cyber Security — Information Protection

Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

The new and modified NERC Glossary Terms Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity shall become effective on the same compliance date as when Reliability Standard CIP-003-6, Requirement R2 is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall

become effective the same compliance date as when Reliability Standard CIP-003-6, Requirement R2 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

9. Standards for Retirement

   Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[1] (Version 5 Plan) remain the same:

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[1] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

~~June 2~~September 3, 2014

Requested Approvals

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel and Training
- CIP-006-6 — Cyber Security — Physical Security
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009–6 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-2 — Cyber Security — Configuration Change Management
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5 — Cyber Security — Personnel and Training
- CIP-006-5 — Cyber Security — Physical Security
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. ~~A Transient Cyber Asset is not a BES Cyber Asset.~~
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. ~~A Transient Cyber Asset is not a Protected Cyber Asset.~~

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	~~Portable media~~Media, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, ~~and/~~or access data. Removable Media are not Cyber Assets. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. ~~A Cyber Asset is not Removable Media.~~
Transient Cyber Asset	A Cyber Asset, directly connected (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not

	limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Low Impact BES Cyber System Electronic Access Point (LEAP)	A Cyber Asset interface that allows Low Impact External Routable Connectivity. The Cyber Asset may reside at a location external to the asset or assets containing low impact BES Cyber Systems. The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System.
Low Impact External Routable Connectivity (LERC)	Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s). Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date that entities must begin to comply that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-6 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the

first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-003-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Requirement R2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 1

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 3

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, element 4

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

2. CIP-004-6 — Cyber Security — Personnel and Training

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three~~six~~ calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-006-6, Requirement R1, Part 1.10

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-6 —Cyber Security — Systems Security Management

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the

first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until ~~six~~ nine calendar months after the effective date of Reliability Standard CIP-007-6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems

Reliability Standard CIP–009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-2 — Cyber Security — Configuration Change Management

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-010-2, Requirement R4

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

7. CIP-011-2 — Cyber Security — Information Protection

   Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

   The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   The new and modified NERC Glossary Terms Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity shall become effective on the same compliance date as when Reliability Standard CIP-003-6, Requirement R2 is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the same compliance date as when Reliability Standard CIP-003-6, Requirement R2 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

9. Standards for Retirement

   Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[1] (Version 5 Plan) remain the same:

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[1] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

September 3, 2014

The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X implementation plan is posted in a clean version although it draws upon the implementation plan from the previous posting and only includes language for those standards balloted as version X.

Requested Approvals

- CIP-003-X — Cyber Security — Security Management Controls
- CIP-004-X — Cyber Security — Personnel and Training
- CIP-007-X — Cyber Security — Systems Security Management
- CIP-010-X — Cyber Security — Configuration Change Management
- CIP-011-X — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5 — Cyber Security — Personnel and Training
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-010-1 — Cyber Security — Configuration Change Management
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

None

General Considerations

The results of the initial CIP V5 Revisions ballot showed industry support for the new communication networks requirements and the removal of the identify, assess, and correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015.

The CIP-003-6 and CIP-010-2 revisions proposed to address the low impact and transient devices directives did not pass initial ballot. As a prudent approach and in order to meet the FERC filing deadline of February 3, 2015 for the two directives, the SDT would like to ballot the IAC revisions on their own without the low impact and transient devices revisions. Assuming the IAC revisions pass the second ballot, these standards can proceed to final ballot along with the communication networks revisions.

The SDT emphasizes that this is NOT an indication that it plans to separate the revision work. Strong progress continues on the low impact and transient devices revisions, and the SDT still hears support from stakeholders to complete all four directive areas of FERC Order No. 791 revisions at the same time. The request for a separate ballot is a practical measure to avoid potential complications with meeting FERC's directive deadlines that, if we were to wait until after the second ballot, time may not allow us to address.

The SDT plans to post a single ballot for the standards that need stakeholder approval for the IAC language removal. These proposed standards will be version X for the ballot. The version X ballot will be posted along with the other revision proposals designated with the appropriate version number. This allows for the simultaneous revision of the standards to address the directive issue areas and when both the version X and the numbered version standards pass ballot, the revisions can be combined into the appropriate numbered standard version.

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date

that entities must begin to comply with that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-X — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-003-X, Requirement R2

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-X, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-X.

2. CIP-004-X — Cyber Security — Personnel and Training

   Reliability Standard CIP-004-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-007-X —Cyber Security — Systems Security Management

   Reliability Standard CIP-007-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the

first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-X, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-X, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-X.

4. CIP-010-X — Cyber Security — Configuration Change Management

Reliability Standard CIP-010-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

5. CIP-011-X — Cyber Security — Information Protection

Reliability Standard CIP-011-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Standards for Retirement

   Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[1] (Version 5 Plan) remain the same:

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[1] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2014-02 CIP Version 5 Revisions – Cyber Security Standards

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the proposed draft CIP standards. The electronic comment form must be completed **by 8 p.m. Eastern on Friday, October 17, 2014**.

All documents and information about this project are available on the project page. If you have questions please contact Marisa Hecht at marisa.hecht@nerc.net or by telephone at 404-446-9620 or Ryan Stewart at ryan.stewart@nerc.net or by telephone at 202-644-8091.

Background Information

On November 22, 2013, FERC issued Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*. In this order, FERC approved version 5 of the CIP standards, and also directed that NERC make the following modifications to those standards:

1. Modify or remove the "identify, assess, and correct" language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for Low Impact assets.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the "identify, assess, and correct" language and communication networks by February 3, 2015, one year from the effective date of FERC Order No. 791. FERC did not place any time frame for NERC to respond to the Low Impact and transient electronic devices directives.

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

Questions

1. For the requirements applicable to Low Impact assets, the Standard Drafting Team (SDT) changed the structure of CIP-003-6, Requirements R1 and R2 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-003-6 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No:

   Comments:

2. The SDT proposed new definitions **Low Impact External Routable Connectivity** and **Low Impact BES Cyber System Electronic Access Point** to clarify the requirement language in CIP-003-6. Do you agree with the proposed new definitions? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

3. For the requirements applicable to transient devices, the SDT changed the structure of CIP-010-2, Requirement R4 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-010-2 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No:

   Comments:

4. The SDT revised the proposed new definitions for Transient Cyber Assets and Removable Media to address issues raised in stakeholder comments. Do you agree with the proposed definitions? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

5. In response to stakeholder comments, the SDT revised the implementation deadlines. The implementation plan now includes tiered deadlines for the aspects of CIP-003-6. The CIP-007-6 timeframe is now consistent with CIP-006-6. Are these timeframes reasonable and appropriate? If not please explain specifically which implementation plan item needs adjusting and include the rationale for the suggested change.

Yes:

No:

Comments:

6. The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.

   In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

   Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

   Yes:

   No:

   Comments:

7. Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP V5 Revisions - Version X Ballot

The results of the initial CIP V5 Revisions ballot showed industry support for the new communication networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015.

The CIP-003-6 and CIP-010-2 revisions proposed to address the low impact and transient devices directives did not pass initial ballot. Stakeholder comments have been addressed by the Standard Drafting Team (SDT) and these standards are being posted for this additional comment and ballot period. However, as a prudent approach and in order to meet the FERC filing deadline of February 3, 2015 for the two directives, the SDT is also balloting the IAC revisions in a separate version of the standards (CIP-003-X and CIP-010-X) without the Low Impact and Transient Devices revisions. In the event that CIP-003-6 or CIP-010-2 do not pass, and the IAC revisions in the version X standards pass, these standards can proceed to final ballot along with the communication networks revisions.

The SDT emphasizes that this is NOT an indication that it plans to separate the revision work. Strong progress continues on the low impact and transient devices revisions, and the SDT still hears support from stakeholders to complete all four directive areas of FERC Order No. 791 revisions at the same time. The request for a separate ballot is a practical measure to avoid potential complications with meeting FERC's directive deadlines that, if we were to wait until after the second ballot, time may not allow us to address.

Posting Plan

The SDT plans to post a single ballot for the standards that need stakeholder approval for the IAC language removal. These proposed standards will be version X for the ballot. The version X ballot will be posted alongside CIP-003-6 and CIP-010 designated with the appropriate version number. This allows for the simultaneous revision of the standards to address the directive issue areas and when both the version X and the numbered version standards pass ballot, the revisions can be combined into the appropriate numbered standard version. The following standards will be posted for ballot of the IAC language removal (proposed redline standards attached):

- CIP-003-X
- CIP-004-X
- CIP-007-X
- CIP-010-X
- CIP-011-X

For CIP-004-X, CIP-007-X, and CIP-011-X, the SDT will not post the version 6 of those standards because they already passed initial ballot. However, since these version 6 standards also contain transient devices revisions, the SDT would like to ballot the version X standards without the revisions addressing transient devices for industry approval on the removal of the IAC language.

The difference between CIP-007-X and CIP-007-6 is the capitalization of "Removable Media" in CIP-007-6. The SDT removed the capitalization in CIP-007-X because should CIP-010-6 fail to pass stakeholder ballot, then the reference to the defined term in CIP-007 would be inaccurate. CIP-007-X also contains the revisions made relative to the

communication networks directive that passed ballot in the initial posting. It is necessary to include both the communication network and IAC revisions in version X of the standard order to have CIP-007 ready for final ballot should the transient device revisions not pass ballot in time.

CIP-011-X removed guidance language references Transient Cyber Assets and Removable Media. CIP-004-X removed language in the requirements that included Transient Cyber Assets and Removable Media.

Stakeholders will be asked to place one vote to approve the IAC language removal from all of the CIP V5 Revision version X standards posted for ballot.

Timing

The Version X revisions will be posted concurrently with the second comment and ballot posting of the low impact and transient devices revisions. See below for the planned balloting schedule.

Ballot Schedule

	Initial Ballot - June 2-July 16	Initial/Addl Ballot - Aug 29-Oct 14	Final Ballot - Oct 31- Nov 10, if all pass **	Final Ballot - Oct 31- Nov 10, if separated***
Version-X*		post		post
CIP-003-6	~ 35%	post	post	
CIP-004-6	passed		post	
CIP-006-6	passed		post	post
CIP-007-6	passed		post	
CIP-009-6	passed		post	post
CIP-010-2	~ 49%	post	post	
CIP-011-2	passed		post	
Definitions - Lows		post	post	
Definitions - TD	passed	post	Post	
IP-V6		post	post	
* Version-X ballot includes: CIP-003, CIP-004, CIP-007, CIP-010, CIP-011, and an implementation plan. CIP-004-6, CIP-007-6 and CIP-011-2 contain reference to the new definitions associated with transient devices.				
** if all revisions pass, the IAC removal will be reflected in the fully revised version posted for final ballot.				
*** If separated, the IAC-X standards will adopt the appropriate version number.				
Schedule is subject to change.				

Implementation Plan

The Implementation Plan deadlines for the IAC requirements will remain effectively unchanged from Version 5 (see posted Version X implementation plan).

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791
September 3, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
106	Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact	The SDT revised Requirements R1 and R2 of CIP-003-6 to include additional specificity regarding the processes that responsible entities must have for low impact BES Cyber Systems. In addition, the SDT developed objective criteria

[2] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 186, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.	surrounding the controls for some entities based on asset-type and routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category. To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility-site level. The SDT confined these revisions in CIP-003-6, Requirements R1 and R2 to the following areas: 1. **Cyber Security Policy:** R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan. 2. **Cyber Security Plan(s):** R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s). The cyber security plan must cover the 4 areas as

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		specified in Attachment 1 of CIP-003-6: a. **Cyber Security Awareness:** Attachment 1, element 1 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices. The SDT determined that adding intervals increases the auditability of the requirement part. b. **Physical Security Controls:** Attachment 1, element 2 and its subparts require controls to restrict physical access to low impact BES Cyber Systems as well as Low Impact BES Cyber System Electronic Access Points (LEAP) used for controlling access as specified in element 3. c. **Electronic Access Controls:** Attachment 1, element 3 and its subparts address protections around Low Impact BES Cyber System External Routable Connectivity (LERC) and Dial-up Connectivity. d. **Cyber Security Incident Response:** Attachment 1, element 4 and its subparts outline the criteria required to be in a Cyber Security Incident response plan.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing.
132	Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it would be unduly burdensome for responsible entities	The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which requires a Transient Cyber Asset and Removable Media plan to provide higher assurance against the propagation of malware when connecting transient devices.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.	The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition. The drafting team determined three distinct scenarios for entities to address in their plan(s) in which transient devices need specific protections: (i) Transient Cyber Assets owned or managed by the Responsible Entity, (ii) Transient Cyber Asset(s) owned or managed by vendors or contractors, and (iii) Removable Media. For Transient Cyber Assets owned or managed by the Responsible Entity, the SDT determined that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management. The controls for this scenario are more specific and recognize the relatively higher frequency in which these devices will be used.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		In the scenario in which contractors or vendors manage the Transient Cyber Assets, the required elements of the plan include those which an entity can verify at the point prior to connecting such as security patch management and malware prevention mechanisms. The security controls entities must apply to Removable Media have considerations for the type of device being protected and include authorization and scanning for malicious code. The Commission provided a list of security controls it expected NERC to consider for addressing transient devices. The consideration of each security element is described as follows: 1. **Device authorization as it relates to users and locations:** CIP-010-2 Requirement R4, Attachment 1 requires entities to authorize Transient Cyber Assets and Removable Media by individual(s) and location(s) prior to connecting them to the BES Cyber System. Vendor or contractor managed Transient Cyber Assets do not have this authorization because the scenario is often single-use and the entity already conducts an inspection and mitigation of the device prior to connection. **2. Software authorization:** The SDT considered controls relating to software authorization but decided against including specific software as part of the authorization performance because such authorization did not

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		contribute meaningfully to cyber security risk reduction. However, software authorization in the form of application whitelisting is provided as an option to mitigate malicious code. **3. Security patch management:** In CIP-010-2 R4, Attachment 1, both entity and vendor/contractor managed devices must have security patch management or other equivalent forms of mitigation to address security vulnerabilities in software. 4. **Malware prevention:** CIP-010-2 Requirement R4, Attachment 1 requires entities to have malware protection on the Transient Cyber Asset (for both entity- and vendor-managed Transient Cyber Assets) and for Removable Media prior to connection. 5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this control and determined this control best applies to entity-managed Transient Cyber Assets with the objective to mitigate the risk of unauthorized use. There are logistical challenges in applying this control to vendor-managed devices, in which the entity likely will have had no control until immediately prior to use. Furthermore, additional guidance is necessary in CIP-011-2 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		devices. The objective to address the unauthorized release of BES Cyber System Information is sufficiently addressed with the requirements in CIP-011-2 to protect and securely handle BES Cyber System Information. 6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-2 requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-2 Requirement R4.
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move	NERC modified the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[3] *See infra* P 223.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	from compliance with the CIP version 3 Standards to the CIP version 5 Standards.4 The Commission agrees that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment	NERC modified the VRF assignment for CIP-004-5.1, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-5, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language. 2. **VSLs for CIP-004-5.1, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-5, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		timeframe contained in the VSLs from 90-210 days to 90-120 days.

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791

~~June 2~~September 3, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
106	Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact	The SDT revised Requirements R1 and R2 of CIP-003-6 to include additional specificity regarding the processes that responsible entities must have for low impact ~~facilities~~BES Cyber Systems. In addition, the SDT developed objective

[2] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 186, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.	criteria surrounding the controls for some entities based on asset-type and ~~routability~~routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category. To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility-site level. The SDT confined these revisions in CIP-003-6, Requirements R1 and R2 to the following ~~four technical~~ areas: 1. **Cyber Security Policy:** R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan. 2. **Cyber Security Plan(s):** R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s). The cyber security plan must cover the 4 areas as

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		specified in Attachment 1 of CIP-003-6: a. **Cyber Security Awareness:** Attachment 1, element 1 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices. The SDT determined that adding intervals increases the auditability of the requirement part. ~~a.~~b. **Physical Security Controls:** Attachment 1, element 2~~.2~~ and its subparts require controls to restrict physical access to ~~L~~low ~~Impact~~ impact BES Cyber Systems ~~and require additional protections for Controls Centers~~as well as Low Impact BES Cyber System Electronic Access Points (LEAP) used for controlling access as specified in element 3. ~~b.~~c. **Electronic Access Controls:** Attachment 1, element ~~2.~~3 and its subparts address protections around ~~external routable protocol paths~~Low Impact BES Cyber System External Routable Connectivity (LERC) and Dial-up Connectivity. ~~c.~~d. **Cyber Security Incident Response:** Attachment 1, element 4~~2.4~~ and its subparts outline the criteria required to be in a Cyber Security

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		Incident response plan. 2. ~~**Cyber Security Awareness:** Part 2.5 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices and Parts 2.2 through 2.4 of Requirement R2. The SDT determined that adding intervals increases the auditability of the requirement part.~~ ~~In addition to the revisions to the four technical areas, the SDT retained the requirement in Part 2.1 to obtain CIP Senior Manager approval of one or more documented policies that address the topics in Parts 2.2 – 2.5.~~
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale	~~NERC proposes to conduct a survey of Cyber Assets, pursuant to Section 1600 of the NERC *Rules of Procedure* (ROP), regarding the scope of the term "BES Cyber Asset." In accordance with Section 1600 of the ROP, NERC may request data or information from Registered Entities that is necessary to meet NERC's obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of FERC's regulations.~~ ~~The purpose of the proposed Data Request is to respond to FERC's directive from Order No. 791 to conduct a survey regarding the scope of the term "BES Cyber Asset" and submit~~

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	~~an informational filing based on the data collected by February 3, 2015.~~ Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing.
132	Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.	The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which requires a Transient Cyber Asset and Removable Media plan to~~includes a set of controls to~~ provide higher assurance against the propagation of malware ~~prior to~~when connecting transient devices. The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition. The drafting team determined three distinct scenarios for entities to address in their plan(s) in which transient devices need specific protections: (i) Transient Cyber Assets owned or

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		managed by the Responsible Entity, (ii) Transient Cyber Asset(s) owned or managed by vendors or contractors, and (iii) Removable Media. For Transient Cyber Assets owned or managed by the Responsible Entity, the SDT determined that entities manage these ~~transient~~ devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management. The controls for this scenario are more specific and recognize the relatively higher frequency in which these devices will be used. In the scenario in which contractors or vendors manage the Transient Cyber Assets, the required elements of the plan include those which an entity can verify at the point prior to connecting such as security patch management and malware prevention mechanisms. The security controls entities must apply to Removable Media have considerations for the type of device being protected and include authorization and scanning for malicious code.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The Commission provided a list of security controls it expecteds NERC to consider for addressing transient devices., and Tthe consideration of each security element is described as follows: 1. **Device authorization as it relates to users and locations:** CIP-010-2 Requirement R4, Part 4.1 Attachment 1 requires entities to authorize Transient Cyber Assets and Removable Media by individual(s) and location(s) prior to connecting them to the BES Cyber System. Vendor or contractor managed Transient Cyber Assets do not have this authorization because the scenario is often single-use and the entity already conducts an inspection and mitigation of the device prior to connection. 2. **Software authorization:** CIP-010-2 Requirement R4, Part 4.1 borrows similar language from CIP-010-2 Requirement R4, Part 1.1 to authorize intentionally installed software on Transient Cyber Assets.The SDT considered controls relating to software authorization but decided against including specific software as part of the authorization performance because such authorization did not contribute meaningfully to cyber security risk reduction. However, software authorization in the form of application whitelisting is provided as an option to mitigate malicious code. 3. **Security patch management:** CIP-010-2 Requirement R4,

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		~~Part 4.7 requires entities to install patches on Transient Cyber Assets and Removable Media, at least once every 35 calendar days, or prior to use, in connecting to the BES Cyber System~~In CIP-010-2 R4, Attachment 1, both entity and vendor/contractor managed devices must have security patch management or other equivalent forms of mitigation to address security vulnerabilities in software. 4. **Malware prevention:** CIP-010-2 Requirement R4, ~~Part 4.2~~Attachment 1 requires entities to have malware protection on the Transient Cyber Asset (for both entity- and vendor-managed Transient Cyber Assets)~~. Requirement R4, Part 4.3 requires malware protectio and n~~ for Removable Media prior to connection~~, and Requirement R4, Part 4.5 requires up-to-date malware signatures~~. 5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this control and determined this control best applies to entity-managed Transient Cyber Assets with the objective to mitigate the risk of unauthorized use. There are logistical challenges in applying this control to vendor-managed devices, in which the entity likely will have had no control until immediately prior to use. Furthermore, A~~a~~the Reliability Standards already

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		~~address the vulnerabilities this control attempts to mitigate, and a~~dditional guidance is necessary in CIP-011-2 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient devices. ~~Specifically, the drafting team determined the two primary objectives in controlling physical access to transient devices are (1) preventing the introduction of malware and (2) preventing the unauthorized release of BES Cyber System Information.~~ The ~~latter~~ objective to address the unauthorized release of BES Cyber System Information is sufficiently addressed with the requirements in CIP-011-2 to protect and securely handle BES Cyber System Information~~. The objective to prevent the introduction of malware is sufficiently addressed through the malware protection requirement proposed for transient devices. Ensuring the physical protection of transient devices outside of the PSP is in some cases more burdensome to the entity than receiving the full protection of the Standard, and has minimal effect to prevent the introduction of malware~~. 6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-2 requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-2 Requirement R4.
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to the CIP version 5 Standards.4 The Commission agrees that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from	NERC modified the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[3] *See infra* P 223.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	NERC modified the VRF assignment for CIP-004-5.1, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-6,

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-5, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language. 2. **VSLs for CIP-004-5.1, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-5, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the timeframe contained in the VSLs from 90-210 days to 90-120 days.

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 (CIP-002-5, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-6 R1	To incorporate a policy or policies for low impact BES Cyber Systems, the main requirement language was modified. "For its high impact and medium impact BES Cyber Systems" was struck from the language as new requirement parts were created. See below for part 1.1 and part 1.2 to see the change justification.
NEW	CIP-003-6 R1.1	"For its high impact and medium impact BES Cyber Systems" was added as a qualifier to the sub-parts below.
CIP-003-5 R1.1	CIP-003-6 R1.1.1	Requirement parts for 1.1 through 1.9 have become 1.1.1 through 1.1.9 with the clarifier added above in part 1.1 of CIP-003-6.
CIP-003-5 R1.2	CIP-003-6 R1.1.2	No change.
CIP-003-5 R1.3	CIP-003-6 R1.1.3	No change.
CIP-003-5 R1.4	CIP-003-6 R1.1.4	No change.
CIP-003-5 R1.5	CIP-003-6 R1.1.5	No change.
CIP-003-5 R1.6	CIP-003-6 R1.1.6	No change.
CIP-003-5 R1.7	CIP-003-6 R1.1.7	No change.
CIP-003-5 R1.8	CIP-003-6 R1.1.8	No change.
CIP-003-5 R1.9	CIP-003-6 R1.1.9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-003-6 R1.2	"For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:" was added as a qualifier to the sub-parts below.
CIP-003-5 R2	CIP-003-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. Furthermore, as the SDT modified its approach of using Attachment 1 instead of the table approach, it modified Requirement R2 to "implement one or more document cyber security plan(s) that include the applicable elements in Attachment 1."
CIP-003-5 R2.1	CIP-003-6 R1.2.1	The security awareness requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.1.
CIP-003-5 R2.2	CIP-003-6, R1.2.2	The physical security controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.2.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.3	CIP-003-6 R1.2.3	The electronic access controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.3. Furthermore, the SDT modified the "external routable protocol connections" as a new definition is being proposed by the SDT for "Low Impact External Routable Connectivity."
CIP-003-5 R2.4	CIP-003-6 R1.2.4	The incident response to a Cyber Security Incident requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.4.
NEW	CIP-003-6, Attachment 1	CIP-003-6 Attachment 1 lists the elements required for low impact asset cyber security plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the lack of objective criteria for Low Impact assets protections.
CIP-003-5 R3	CIP-003-6 R3	No change.
CIP-003-5 R4	CIP-003-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-6 R1	No change.
CIP-004-5.1 R1.1	CIP-004-6 R1.1	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2	CIP-004-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken. The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement “a cyber security training program(s).” That modification was made for clarity and consistency across the standards.
CIP-004-5.1 R2.1	CIP-004-6 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-6 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-6 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-6 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-6 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-6 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-6 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-6 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-6 R2.1.8	No change.
CIP-004-5.1 R2.1.9	CIP-004-6 R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity’s cyber security training program. The training must address cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.
CIP-004-5.1 R2.2	CIP-004-6 R2.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.3	CIP-004-6 R2.3	No change.
CIP-004-5.1 R3	CIP-004-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R3.1	CIP-004-6 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-6 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-6 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-6 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-6 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-6 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-6 R3.5	No change.
CIP-004-5.1 R4	CIP-004-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R4.1	CIP-004-6 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-6 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-6 R4.1.2	No change.
CIP-004-5.1 R4.1.3	CIP-004-6 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-6 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-6 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-6 R4.4	No change.
CIP-004-5.1 R5	CIP-004-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R5.1	CIP-004-6 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-6 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-6 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-6 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-6 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-6 R1.1	No change.
CIP-007-5 R1.2	CIP-007-6 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-6 R2.1	No change.
CIP-007-5 R2.2	CIP-007-6 R2.2	No change.
CIP-007-5 R2.3	CIP-007-6 R2.3	No change.
CIP-007-5 R2.4	CIP-007-6 R2.4	No change.
CIP-007-5 R3	CIP-007-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R3.1	CIP-007-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.2	CIP-007-6 R3.2	No change.
CIP-007-5 R3.3	CIP-007-6 R3.3	No change.
CIP-007-5 R4	CIP-007-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R4.1	CIP-007-6 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-6 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-6 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-6 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-6 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-6 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-6 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-6 R4.3	No change.
CIP-007-5 R4.4	CIP-007-6 R4.4	No change.
CIP-007-5 R5	CIP-007-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R4	CIP-007-6 R4	No change.
CIP-007-5 R5	CIP-007-6 R5	No change.
CIP-007-5 R5.1	CIP-007-6 R5.1	No change.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.4	CIP-007-6 R5.4	No change.
CIP-007-5 R5.5	CIP-007-6 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-6 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-6 R5.5.2	No change.
CIP-007-5 R6	CIP-007-6 R6	No change.
CIP-007-5 R7	CIP-007-6 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-2 R1.1	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-2 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-2 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-2 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-2 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-2 R1.5.2	No change.
CIP-010-1 R2	CIP-010-2 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-2 R2.1	No change.
CIP-010-1 R3	CIP-010-2 R3	No change.
CIP-010-1 R3.1	CIP-010-2 R3.1	No change.
CIP-010-1 R3.2	CIP-010-2 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-2 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-2 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-2 R3.3	No change.
CIP-010-1 R3.4	CIP-010-2 R3.4	No change.
NEW	CIP-010-2 R4	To respond to the FERC Order No. 791 directive to address transient devices, the SDT modified its approach to use Attachment 1 instead of the table approach. It modified Requirement R4 to "implement one or more documented plan(s) for Transient Cyber Asset and Removable Media that include the applicable elements in Attachment 1, except under CIP Exceptional Circumstances."
NEW	CIP-010-2, Attachment 1	CIP-010-2 Attachment 1 lists the elements required for Transient Cyber Asset and Removable Media Plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the risks posed by transient devices.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-2 R1.1	No change.
CIP-011-1 R1.2	CIP-011-2 R1.2	No change.
CIP-011-1 R2	CIP-011-2 R2	No change.
CIP-011-1 R2.1	CIP-011-2 R2.1	No change.
CIP-011-1 R2.2	CIP-011-2 R2.2	No change.

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 (CIP-002-5, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-6 R1	~~No change.~~ To incorporate a policy or policies for low impact BES Cyber Systems, the main requirement language was modified. "For its high impact and medium impact BES Cyber Systems" was struck from the language as new requirement parts were created. See below for part 1.1 and part 1.2 to see the change justification.
~~CIP-003-5 R1.1~~NEW	CIP-003-6 R1.1	~~No change.~~ "For its high impact and medium impact BES Cyber Systems" was added as a qualifier to the sub-parts below.
CIP-003-5 R1.1	CIP-003-6 R1.1.1	Requirement parts for 1.1 through 1.9 have become 1.1.1 through 1.1.9 with the clarifier added above in part 1.1 of CIP-003-6.
CIP-003-5 R1.2	CIP-003-6 ~~R1.2~~R1.1.2	No change.
CIP-003-5 R1.3	CIP-003-6 ~~R1.3~~R1.1.3	No change.
CIP-003-5 R1.4	CIP-003-6 ~~R1.4~~R1.1.4	No change.
CIP-003-5 R1.5	CIP-003-6 ~~R1.5~~R1.1.5	No change.
CIP-003-5 R1.6	CIP-003-6 ~~R1.6~~R1.1.6	No change.
CIP-003-5 R1.7	CIP-003-6 ~~R1.7~~R1.1.7	No change.
CIP-003-5 R1.8	CIP-003-6 ~~R1.8~~R1.1.8	No change.
CIP-003-5 R1.9	CIP-003-6 ~~R1.9~~R1.1.9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-003-6 R1.2	"For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:" was added as a qualifier to the sub-parts below.
CIP-003-5 R2	CIP-003-6 R2~~, CIP-003-6, R2.1~~	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. Furthermore, as the SDT modified its approach of using Attachment 1 instead of the table approach, it modified Requirement R2 to "implement one or more document cyber security plan(s) that include the applicable elements in Attachment 1." ~~The main requirement was modified to follow a similar structure to parent Requirements of those requirement parts in the table format.~~ ~~The CIP Senior Manager review and approval at least once every 15 months was mapped to CIP-003-6 R2.1.~~
CIP-003-5 R2.1	~~CIP-003-6 R2.6~~ CIP-003-6 R1.2.1	The security awareness requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.1. ~~The security awareness requirement part was mapped to Part 2.6 to reinforce cyber security practices at least quarterly, while addressing Parts 2.2 through 2.5 once every 15 calendar months. This added objective criteria to security awareness, while not to the rigor of Medium and High BES Cyber Systems.~~

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.2	~~CIP-003-6 R2.2~~ CIP-003-6, R1.2.2	The physical security controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.2. ~~Expanding the physical security controls, Part 2.2 addresses operational or procedural control(s) to restrict physical access.~~
~~NEW~~	~~CIP-003-6 R2.3~~	~~Expanding the physical security controls, Part 2.3 requires implementation of processes to include Parts 2.3.1 and 2.3.2 for low impact BES Cyber Systems at Control Centers.~~
~~NEW~~	~~CIP-003-6 R2.3.1~~	~~Expanding the physical security controls, Part 2.3.1 addresses escorted access of visitors at Control Centers.~~
~~NEW~~	~~CIP-003-6 R2.3.2~~	~~Expanding the physical security controls, Part 2.3.2 addresses monitored physical access point(s) at Control Centers with external routable protocol paths.~~
CIP-003-5 R2.3	~~CIP-003-6 R2.4~~ CIP-003-6 R1.2.3	The electronic access controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.3. Furthermore, the SDT modified the "external routable protocol connections" as a new definition is being proposed by the SDT for "Low Impact External Routable Connectivity." ~~The electronic access controls were added as Part 2.4. The documented process(es) collectively must include Parts 2.4.1 through 2.4.3.~~

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
~~NEW~~	~~CIP-003-6 R2.4.1~~	~~Expanding the electronic access controls, Part 2.4.1 addresses all external routable protocol paths, if any, as needing to be through one or more identified access point(s).~~
~~NEW~~	~~CIP-003-6 R2.4.2~~	~~Expanding the electronic access controls, Part 2.4.2 addresses requiring inbound and outbound access permissions for each identified access point, including the reason for granting access, and deny all other access by default.~~
~~NEW~~	~~CIP-003-6 R2.4.3~~	~~Expanding the electronic access controls, Part 2.4.3 addresses authentication when establishing Dial-Up Connectivity, per Cyber Asset capability.~~
CIP-003-5 R2.4	~~CIP-003-6 R2.5~~ CIP-003-6 R1.2.4	The incident response to a Cyber Security Incident requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.4. ~~The incident response to a Cyber Security Incident requirement part remains in Part 2.5. The documented response plan(s) collectively must include Parts 2.5.1 through 2.5.6.~~
~~NEW~~	~~CIP-003-6 R2.5.1~~	~~Expanding the incident response controls, Part 2.5.1 address the identification, classification, and response to Cyber Security Incidents.~~
~~NEW~~	~~CIP-003-6 R2.5.2~~	~~Expanding the incident response controls, Part 2.5.2 addresses whether an identified Cyber Security Incident is reportable.~~
~~NEW~~	~~CIP-003-6 R2.5.3~~	~~Expanding the incident response controls, Part 2.5.3 addresses the notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center.~~

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
~~NEW~~	~~CIP-003-6 R2.5.4~~	~~Expanding the incident response controls, Part 2.5.4 addresses the roles and responsibilities of Cyber Security Incident response groups or individuals.~~
~~NEW~~	~~CIP-003-6 R2.5.5~~	~~Expanding the incident response controls, Part 2.5.5 addresses the incident handling procedures for Cyber Security Incidents.~~
~~NEW~~	~~CIP-003-6 R2.5.6~~	~~Expanding the incident response controls, Part 2.5.6 addresses the testing of the plan(s) at least once per 36 calendar months.~~
NEW	CIP-003-6, Attachment 1	CIP-003-6 Attachment 1 lists the elements required for low impact asset cyber security plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the lack of objective criteria for Low Impact assets protections.
CIP-003-5 R3	CIP-003-6 R3	No change.
CIP-003-5 R4	CIP-003-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-6 R1	No change.
CIP-004-5.1 R1.1	CIP-004-6 R1.1	No change.
CIP-004-5.1 R2	CIP-004-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement "a cyber security training program(s)." That modification was made for clarity and consistency across the standards.
CIP-004-5.1 R2.1	CIP-004-6 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-6 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-6 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-6 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-6 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-6 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-6 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-6 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-6 R2.1.8	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.1.9	CIP-004-6 R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity's cyber security training program. The training must address cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.
CIP-004-5.1 R2.2	CIP-004-6 R2.2	No change.
CIP-004-5.1 R2.3	CIP-004-6 R2.3	No change.
CIP-004-5.1 R3	CIP-004-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-004-5.1 R3.1	CIP-004-6 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-6 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-6 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-6 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-6 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-6 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-6 R3.5	No change.
CIP-004-5.1 R4	CIP-004-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.
CIP-004-5.1 R4.1	CIP-004-6 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-6 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-6 R4.1.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R4.1.3	CIP-004-6 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-6 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-6 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-6 R4.4	No change.
CIP-004-5.1 R5	CIP-004-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R5.1	CIP-004-6 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-6 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-6 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-6 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-6 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-6 R1.1	No change.
CIP-007-5 R1.2	CIP-007-6 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-6 R2.1	No change.
CIP-007-5 R2.2	CIP-007-6 R2.2	No change.
CIP-007-5 R2.3	CIP-007-6 R2.3	No change.
CIP-007-5 R2.4	CIP-007-6 R2.4	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3	CIP-007-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R3.1	CIP-007-6 R3.1	No change.
CIP-007-5 R3.2	CIP-007-6 R3.2	No change.
CIP-007-5 R3.3	CIP-007-6 R3.3	No change.
CIP-007-5 R4	CIP-007-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R4.1	CIP-007-6 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-6 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-6 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-6 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-6 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-6 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-6 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-6 R4.3	No change.
CIP-007-5 R4.4	CIP-007-6 R4.4	No change.
CIP-007-5 R5	CIP-007-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R4	CIP-007-6 R4	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5	CIP-007-6 R5	No change.
CIP-007-5 R5.1	CIP-007-6 R5.1	No change.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R5.4	CIP-007-6 R5.4	No change.
CIP-007-5 R5.5	CIP-007-6 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-6 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-6 R5.5.2	No change.
CIP-007-5 R6	CIP-007-6 R6	No change.
CIP-007-5 R7	CIP-007-6 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-2 R1.1	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-2 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-2 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-2 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-2 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-2 R1.5.2	No change.
CIP-010-1 R2	CIP-010-2 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-2 R2.1	No change.
CIP-010-1 R3	CIP-010-2 R3	No change.
CIP-010-1 R3.1	CIP-010-2 R3.1	No change.
CIP-010-1 R3.2	CIP-010-2 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-2 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-2 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-2 R3.3	No change.
CIP-010-1 R3.4	CIP-010-2 R3.4	No change.
NEW	CIP-010-2 R4	To respond to the FERC Order No. 791 directive to address transient devices, the SDT modified its approach to use Attachment 1 instead of the table approach. It modified Requirement R4 to "implement one or more documented plan(s) for Transient Cyber Asset and Removable Media ~~plan(s)~~ that include the applicable elements in Attachment 1, except under CIP Exceptional Circumstances."~~new the revised Requirement R4 from the last posting follows a similar approach to the proposed CIP-003-6 attachment. follows the table format to ensure Registered Entities implemented one or more documented process(es) that collectively include each of the applicable parts in CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection.~~ ~~All of the new Requirement Parts under Requirement R4 are in response to this directive.~~
NEW	CIP-010-2, Attachment 1	CIP-010-2 Attachment 1 lists the elements required for Transient Cyber Asset and Removable Media Plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the risks posed by transient devices.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
~~NEW~~	~~CIP-010-2 R4.1~~	~~Part 4.1 ensures Responsible Entities authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. The authorization shall include the Requirement Parts 4.1.1 through 4.1.4.~~
~~NEW~~	~~CIP-010-2 R4.1.1~~	~~Authorization shall include users, individually or by group/role.~~
~~NEW~~	~~CIP-010-2 R4.1.2~~	~~Authorization shall include locations, individually or by group/role.~~
~~NEW~~	~~CIP-010-2 R4.1.3~~	~~Authorization shall include defined acceptable use.~~
~~NEW~~	~~CIP-010-2 R4.1.4~~	~~Authorization shall include operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).~~
~~NEW~~	~~CIP-010-2 R4.2~~	~~Part 4.2 ensures Responsible Entities use method(s) to deter, detect, or prevent malicious code introduction on Transient Cyber Assets (per Cyber Asset capability).~~
	~~CIP-010-2 R4.3~~	~~Part 4.3 ensures Responsible Entities use method(s) to detect malicious code on Removable Media prior to use on applicable systems.~~
~~NEW~~	~~CIP-010-2 R4.4~~	~~Part 4.4 ensures Responsible Entities mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.~~
~~NEW~~	~~CIP-010-2 R4.5~~	~~Part 4.5 ensures Responsible Entities update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.~~
~~NEW~~	~~CIP-010-2 R4.6~~	~~Part 4.6 ensures Responsible Entities evaluate Transient Cyber Assets prior to use for modifications that deviate from Part 4.1.4.~~
~~NEW~~	~~CIP-010-2 R4.7~~	~~Part 4.7 ensures Responsible Entities evaluate Transient Cyber Assets periodically to ensure security patches are up-to-date.~~

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-2 R1.1	No change.
CIP-011-1 R1.2	CIP-011-2 R1.2	No change.
CIP-011-1 R2	CIP-011-2 R2	No change.
CIP-011-1 R2.1	CIP-011-2 R2.1	No change.
CIP-011-1 R2.2	CIP-011-2 R2.2	No change.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement Reminder

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Additional Ballots Now Open through October 17, 2014

Now Available

Additional ballots for the standards, definitions, implementation plans for **Critical Infrastructure Protection Standards Version 5 Revisions** and non-binding polls of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) are open through **8 p.m. Eastern on Friday, October 17, 2014.**

The open ballots are as follows:

- Project 2014-02 CIP-003-6
- Project 2014-02 CIP-010-2
- Project 2014-02 CIP Version X*
- Project 2014-02 Definition CIP-003-6
- Project 2014-02 Definition CIP-010-2
- Project 2014-02 CIP Implementation Plan*
- 7 Non-Binding Polls of the associated VRFs and VSLs

*Please note that the Project 2014-02 CIP Version X ballot includes the Version X Reliability Standards and Version X Implementation Plan whereas the Project 2014-02 Implementation Plan ballot includes the Implementation Plan posted for CIP-003-6 and CIP-010-2.

Background information for this project can be found on the project page.

Instructions for Balloting

Members of the ballot pools associated with this project may log in and submit their vote for the standards, definitions, implementation plans and associated VRFs and VSLs by clicking here.

Note: If a member cast a vote in the initial ballot, that vote will not carry over to the additional ballot. It is the responsibility of the registered voter in the ballot pool to cast a vote again in the additional ballot. To ensure a quorum is reached, if you do not want to vote affirmative or negative, please cast an abstention.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standards and post them for an additional ballot. If the comments do not show the need for significant revisions, the standards will proceed to a final ballot**.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

If you have questions please contact Ryan Stewart or Marisa Hecht.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement Reminder

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Additional Ballots Now Open through October 17, 2014

Now Available

Additional ballots for the standards, definitions, implementation plans for **Critical Infrastructure Protection Standards Version 5 Revisions** and non-binding polls of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) are open through **8 p.m. Eastern on Friday, October 17, 2014.**

The open ballots are as follows:

- Project 2014-02 CIP-003-6
- Project 2014-02 CIP-010-2
- Project 2014-02 CIP Version X*
- Project 2014-02 Definition CIP-003-6
- Project 2014-02 Definition CIP-010-2
- Project 2014-02 CIP Implementation Plan*
- 7 Non-Binding Polls of the associated VRFs and VSLs

*Please note that the Project 2014-02 CIP Version X ballot includes the Version X Reliability Standards and Version X Implementation Plan whereas the Project 2014-02 Implementation Plan ballot includes the Implementation Plan posted for CIP-003-6 and CIP-010-2.

Background information for this project can be found on the project page.

Instructions for Balloting

Members of the ballot pools associated with this project may log in and submit their vote for the standards, definitions, implementation plans and associated VRFs and VSLs by clicking here.

Note: If a member cast a vote in the initial ballot, that vote will not carry over to the additional ballot. It is the responsibility of the registered voter in the ballot pool to cast a vote again in the additional ballot. To ensure a quorum is reached, if you do not want to vote affirmative or negative, please cast an abstention.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standards and post them for an additional ballot. If the comments do not show the need for significant revisions, the standards will proceed to a final ballot**.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

If you have questions please contact Ryan Stewart or Marisa Hecht.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Formal Comment Period Now Open through October 17, 2014

Now Available

A 45-day formal comment period for **Critical Infrastructure Protection Standards Version 5 Revisions** is open through **8 p.m. Eastern on Friday, October 17, 2014.**

Background information for this project can be found on the project page.

Instructions for Commenting

Please use the electronic form to submit comments on the standards. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

Additional ballots for the standards, definitions and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **October 8-17, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

If you have questions please contact Ryan Stewart or Marisa Hecht.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Additional Ballot and Non-Binding Poll Results

Now Available

Additional ballots for CIP Version X, CIP-003-6, CIP-010-2 - **Critical Infrastructure Protection Version 5 Revisions**, two definitions, one implementation plan, and seven non-binding polls of the associated Violation Risk Factors and Violation Severity Levels concluded at **8 p.m. Eastern, Friday, October 17, 2014**.

Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballots.

Ballot	Quorum /Approval
CIP Version X	84.63% / 93.21%
CIP-003-6	84.15% / 68.09%
CIP-010-2	84.15% / 74.25%
Definition CIP-003-6	83.90% / 79.91%
Definition CIP-010-2	83.41% / 85.68%
Implementation Plan	83.66% / 89.01%

Non-Binding Poll	Quorum/Supportive Opinions
CIP-003-X	83.96% / 91.79%
CIP-003-6	84.49% / 81.34%
CIP-004-X	83.96% / 96.63%
CIP-007-X	83.96% / 96.63%
CIP-010-X	84.22% / 95.52%
CIP-010-2	84.49% / 85.93%

Non-Binding Poll	Quorum/Supportive Opinions
CIP-011-X	84.22% / 98.13%

Background information for this project can be found on the project page.

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standards and post them for an additional ballot. If the comments do not show the need for significant revisions, the standards will proceed to a final ballot.

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact either Marisa Hecht or Ryan Stewart.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2014-02 CIP Version X
Ballot Period:	10/8/2014 - 10/17/2014
Ballot Type:	Successive
Total # Votes:	347
Total Ballot Pool:	410
Quorum:	**84.63 % The Quorum has been reached**
Weighted Segment Vote:	93.21 %
Ballot Results:	**The Ballot has Closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	87	0.946	5	0.054	0	2	19
2 - Segment 2	9	0.9	9	0.9	0	0	0	0	0
3 - Segment 3	93	1	72	0.889	9	0.111	0	3	9
4 - Segment 4	34	1	20	0.833	4	0.167	0	3	7
5 - Segment 5	91	1	65	0.915	6	0.085	0	2	18
6 - Segment 6	54	1	43	0.935	3	0.065	0	2	6
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.7	7	0.7	0	0	0	0	0
Totals	**410**	**7.1**	**308**	**6.618**	**27**	**0.482**	**0**	**12**	**63**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	

1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by Nebraska Public Power District)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dave Burkey, Puget Sound Energy)
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	

1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED

3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	COMMENT RECEIVED
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	

3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	

5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	

5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		

6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-003-6
Ballot Period:	10/8/2014 - 10/17/2014
Ballot Type:	Successive
Total # Votes:	345
Total Ballot Pool:	410
Quorum:	**84.15 % The Quorum has been reached**
Weighted Segment Vote:	68.09 %
Ballot Results:	**The Ballot has Closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	61	0.67	30	0.33	0	1	21
2 - Segment 2	9	0.5	3	0.3	2	0.2	0	4	0
3 - Segment 3	93	1	53	0.646	29	0.354	0	1	10
4 - Segment 4	34	1	17	0.68	8	0.32	0	2	7
5 - Segment 5	91	1	42	0.583	30	0.417	0	1	18
6 - Segment 6	54	1	28	0.583	20	0.417	0	1	5
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**6.7**	**215**	**4.562**	**120**	**2.138**	**0**	**10**	**65**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	COMMENT RECEIVED
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	COMMENT RECEIVED
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Kalem Long)
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Negative	COMMENT RECEIVED
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	

1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Negative	COMMENT RECEIVED
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
1	MidAmerican Energy Co.	Terry Harbour	Negative	COMMENT RECEIVED
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by Nebraska Public Power District)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC and NYPA)
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe Obrien NIPSCO)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas E. Foltz, American Electric Power)
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		

1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dave Burkey, Puget Sound Energy)
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patrick Farrell)
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI and NPCC)
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Amy Casuscelli, Xcel Energy)
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Leonard Kula	Negative	COMMENT RECEIVED
2	ISO New England, Inc.	Matthew F Goldberg	Abstain	

2	MISO	Marie Knox	Abstain	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Abstain	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon/Exelon)
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion's)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Negative	COMMENT RECEIVED
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Negative	COMMENT RECEIVED
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	COMMENT RECEIVED
3	New York Power Authority	David R Rivera	Negative	COMMENT RECEIVED
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien)
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Negative	COMMENT RECEIVED
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	

3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Negative	SUPPORTS THIRD PARTY COMMENTS - (As filed by Patrick Farrell on behalf of SCE)
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI Comments)
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (Please see TVA's comments submitted through the electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	COMMENT RECEIVED
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group and FMPA)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	

4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo Wisconsin Electric)
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Negative	COMMENT RECEIVED
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Standifur)
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (CLIFF JOHNSON)
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike I kidwell		
				SUPPORTS THIRD

5	Entergy Services, Inc.	Tracey Stubbs	Negative	PARTY COMMENTS - (Entergy CIP)
5	Exelon Nuclear	Mark F Draper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon / Exelon)
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Negative	COMMENT RECEIVED
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC comments)
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support Joe O'Brien's comments on behalf of Jerry Freese.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	

5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Puget Sound Energy)
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Negative	COMMENT RECEIVED
5	Southern Company Generation	William D Shultz	Negative	COMMENT RECEIVED
5	Southern Indiana Gas and Electric Co.	Rob Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Third Party Comments - EEI)
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	COMMENT RECEIVED
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Negative	COMMENT RECEIVED
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (AEP Comments)
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Austin Energy)
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon/Exelon)
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Negative	COMMENT RECEIVED
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC)
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments filed by Patrick Farrel on behalf of SCE)
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support comments submitted by EEI)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Negative	COMMENT

				RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Negative	COMMENT RECEIVED
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-010-2
Ballot Period:	10/8/2014 - 10/17/2014
Ballot Type:	Successive
Total # Votes:	345
Total Ballot Pool:	410
Quorum:	**84.15 % The Quorum has been reached**
Weighted Segment Vote:	74.25 %
Ballot Results:	**The Ballot has Closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	69	0.758	22	0.242	0	1	21
2 - Segment 2	9	0.9	6	0.6	3	0.3	0	0	0
3 - Segment 3	93	1	56	0.709	23	0.291	0	4	10
4 - Segment 4	34	1	19	0.792	5	0.208	0	3	7
5 - Segment 5	91	1	47	0.671	23	0.329	0	3	18
6 - Segment 6	54	1	32	0.667	16	0.333	0	1	5
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**7**	**239**	**5.197**	**93**	**1.803**	**0**	**13**	**65**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	COMMENT RECEIVED
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	

1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
1	MidAmerican Energy Co.	Terry Harbour	Negative	COMMENT RECEIVED
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (National Grid supports NPCC's comments.)
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Affirmative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Negative	SUPPORTS THIRD PARTY COMMENTS - (CIte NPCC)
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe Obrien NIPSCO)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas E. Foltz, American Electric Power)
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	

1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dave Burkey, Puget Sound Energy)
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI and NPCC)
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Negative	COMMENT RECEIVED
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	COMMENT RECEIVED
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Abstain	
3	APS	Sarah Kist	Affirmative	

3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion's)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Negative	COMMENT RECEIVED
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (GPC)
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
3	Nebraska Public Power District	Tony Eddleman	Negative	COMMENT RECEIVED
3	New York Power Authority	David R Rivera	Negative	COMMENT RECEIVED
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien)
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Negative	COMMENT RECEIVED
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI Comments)
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (Please see TVA's comments submitted through the electronic comment form)

3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	COMMENT RECEIVED
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group and FMPA)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy's Comments)
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo Wisconsin Electric)
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
				SUPPORTS THIRD PARTY

5	BC Hydro and Power Authority	Clement Ma	Negative	COMMENTS - (Patrica Robertson)
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy's Comments)
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(GPC)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC comments)
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support Joe O'Brien's comments on behalf of Jerry Freese.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Puget Sound Energy)
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	COMMENT RECEIVED
5	Southern Indiana Gas and Electric Co.	Rob Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Third Party Comments - EEI)
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		

5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	COMMENT RECEIVED
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (AEP Comments)
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC)
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	

6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support comments submitted by EEI)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Ballot Results	
Ballot Name:	Project 2014-02 Definition CIP-003-6
Ballot Period:	10/8/2014 - 10/17/2014
Ballot Type:	Successive
Total # Votes:	344
Total Ballot Pool:	410
Quorum:	**83.90 % The Quorum has been reached**
Weighted Segment Vote:	79.91 %
Ballot Results:	**The Ballot has Closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	70	0.787	19	0.213	0	2	22
2 - Segment 2	9	0.4	3	0.3	1	0.1	0	5	0
3 - Segment 3	93	1	67	0.807	16	0.193	0	0	10
4 - Segment 4	34	1	20	0.833	4	0.167	0	3	7
5 - Segment 5	91	1	51	0.718	20	0.282	0	2	18
6 - Segment 6	54	1	35	0.729	13	0.271	0	1	5
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**6.6**	**257**	**5.274**	**74**	**1.326**	**0**	**13**	**66**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Negative	COMMENT RECEIVED
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED

1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
1	MidAmerican Energy Co.	Terry Harbour	Negative	COMMENT RECEIVED
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by Nebraska Public Power District)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White		
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe Obrien NIPSCO)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas E. Foltz, American Electric Power)
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dave Burkey, Puget Sound Energy)
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	

1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Amy Casuscelli, Xcel Energy)
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Leonard Kula	Negative	COMMENT RECEIVED
2	ISO New England, Inc.	Matthew F Goldberg	Abstain	
2	MISO	Marie Knox	Abstain	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Abstain	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Abstain	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	

3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion's)
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	COMMENT RECEIVED
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien)
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's

				Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Negative	COMMENT RECEIVED
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI Comments)
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (Please see TVA's comments submitted through the electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	COMMENT RECEIVED
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
				SUPPORTS

4	Herb Schrayshuen	Herb Schrayshuen	Negative	THIRD PARTY COMMENTS - (NPCC)
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo Wisconsin Electric)
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Negative	COMMENT RECEIVED
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (CLIFF JOHNSON)
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		

5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Negative	SUPPORTS THIRD PARTY COMMENTS - (Entergy CIP)
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	COMMENT RECEIVED
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	Nevada Power Co.	Richard Salgo	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support Joe O'Brien's comments on behalf of Jerry Freese.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Puget Sound Energy)
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	

5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	COMMENT RECEIVED
5	Southern Indiana Gas and Electric Co.	Rob Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Third Party Comments - EEI)
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	COMMENT RECEIVED
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Negative	COMMENT RECEIVED
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (AEP Comments)
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	

6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support comments submitted by EEI)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Negative	COMMENT RECEIVED
6	Xcel Energy, Inc.	Peter Colussy	Negative	COMMENT RECEIVED
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 Definition CIP-010-2
Ballot Period:	10/8/2014 - 10/17/2014
Ballot Type:	Successive
Total # Votes:	342
Total Ballot Pool:	410
Quorum:	**83.41 % The Quorum has been reached**
Weighted Segment Vote:	85.68 %
Ballot Results:	**The Ballot has Closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	75	0.843	14	0.157	0	1	23
2 - Segment 2	9	0.9	7	0.7	2	0.2	0	0	0
3 - Segment 3	93	1	67	0.838	13	0.163	0	3	10
4 - Segment 4	34	1	21	0.875	3	0.125	0	3	7
5 - Segment 5	91	1	57	0.814	13	0.186	0	2	19
6 - Segment 6	54	1	39	0.813	9	0.188	0	1	5
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.7	7	0.7	0	0	0	0	0
Totals	**410**	**7.1**	**278**	**6.083**	**54**	**1.019**	**0**	**10**	**68**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	COMMENT RECEIVED
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	

1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Affirmative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White		
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe Obrien NIPSCO)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas E. Foltz, American Electric Power)
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dave Burkey, Puget Sound Energy)
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	

1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Negative	COMMENT RECEIVED
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Abstain	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		

3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Negative	COMMENT RECEIVED
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien)
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
				COMMENT

3	Puget Sound Energy, Inc.	Mariah R Kennedy	Negative	RECEIVED
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI Comments)
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	COMMENT RECEIVED
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy's Comments)
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	

4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo Wisconsin Electric)
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patricia Robertson)
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergy's comments)
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
	Massachusetts Municipal Wholesale Electric			COMMENT

5	Company	David Gordon	Negative	RECEIVED
5	MEAG Power	Steven Grego	Negative	SUPPORTS THIRD PARTY COMMENTS - (GPC)
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support Joe O'Brien's comments on behalf of Jerry Freese.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Puget Sound Energy)
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	COMMENT RECEIVED
5	Southern Indiana Gas and Electric Co.	Rob Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Third Party Comments - EEI)
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Affirmative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	COMMENT RECEIVED
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		

6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (AEP Comments)
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Tacoma Public Utilities	Michael C Hill	Affirmative	

6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support comments submitted by EEI)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Ballot Results	
Ballot Name:	Project 2014-02 CIP Implementation Plan
Ballot Period:	10/8/2014 - 10/17/2014
Ballot Type:	Successive
Total # Votes:	343
Total Ballot Pool:	410
Quorum:	**83.66 % The Quorum has been reached**
Weighted Segment Vote:	89.01 %
Ballot Results:	**The Ballot has Closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	72	0.847	13	0.153	0	6	22
2 - Segment 2	9	0.8	7	0.7	1	0.1	0	1	0
3 - Segment 3	93	1	71	0.899	8	0.101	0	4	10
4 - Segment 4	34	1	23	0.958	1	0.042	0	3	7
5 - Segment 5	91	1	60	0.857	10	0.143	0	3	18
6 - Segment 6	54	1	40	0.87	6	0.13	0	2	6
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.1	1	0.1	0	0	0	0	1

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**7**	**284**	**6.231**	**40**	**0.769**	**0**	**19**	**67**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz AEP)
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Abstain	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	

1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	COMMENT RECEIVED
1	Minnesota Power, Inc.	Randi K. Nyholm	Abstain	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support SPP Comments)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White		
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas E. Foltz, American Electric Power)
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dave Burkey, Puget Sound Energy)
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED

1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	COMMENT RECEIVED
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	

3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool (SPP) comment)
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Negative	COMMENT RECEIVED
3	Rutherford EMC	Thomas Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	

3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		

5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Puget Sound Energy)

5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	COMMENT RECEIVED
5	Southern Indiana Gas and Electric Co.	Rob Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support Third Party Comments - EEI)
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (AEP Comments)
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	

6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-003-X
Poll Period:	10/8/2014 - 10/17/2014
Total # Opinions:	314
Total Ballot Pool:	374
Summary Results:	83.96% of those who registered to participate provided an opinion or an abstention; 91.79% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		

1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Abstain	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Negative	COMMENT RECEIVED
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Negative	SUPPORTS THIRD PARTY COMMENTS - (cite NYPA and NPCC)
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	

1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	

1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Abstain	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Abstain	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED-Cliff Johnson
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	

3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Negative	COMMENT RECEIVED
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED

3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Abstain	

5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Negative	COMMENT RECEIVED
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (CLIFF JOHNSON)
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden		
5	Entergy Services, Inc.	Tracey Stubbs	Negative	SUPPORTS THIRD PARTY COMMENTS - (Entergy CIP)
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	

5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Negative	COMMENT RECEIVED
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	

5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Negative	COMMENT RECEIVED
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		

6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-003-6
Poll Period:	10/8/2014 - 10/17/2014
Total # Opinions:	316
Total Ballot Pool:	374
Summary Results:	84.49% of those who registered to participate provided an opinion or an abstention; 81.34% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	

1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Abstain	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Negative	COMMENT RECEIVED
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	COMMENT RECEIVED
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cite NYPA and NPCC)
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		

1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe Obrien NIPSCO)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Negative	SUPPORTS THIRD PARTY COMMENTS - (Patrick Farrell)
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	

1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Abstain	
2	MISO	Marie Knox	Abstain	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Abstain	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	

3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED - Cliff Johnson
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Negative	COMMENT RECEIVED
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Negative	COMMENT RECEIVED
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Joe O'Brien)
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Negative	SUPPORTS THIRD PARTY COMMENTS - (Filed by Patrick Farrell on behalf of SCE)
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI Comments)
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	

4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cliff Johnson)
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo Wisconsin Electric)
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	

5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (CLIFF JOHNSON)
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	EDP Renewables North America LLC	Heather Bowden		
5	Entergy Services, Inc.	Tracey Stubbs	Negative	SUPPORTS THIRD PARTY COMMENTS - (Entergy CIP)
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Negative	COMMENT RECEIVED
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	

5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC comments)
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support Joe O'Brien's comments on behalf of Jerry Freese.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Negative	COMMENT RECEIVED

5	Southern Company Generation	William D Shultz	Negative	COMMENT RECEIVED
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Abstain	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Negative	COMMENT RECEIVED
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Negative	COMMENT RECEIVED
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC)
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED

6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments filed by Patrick Farrel on behalf of SCE)
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support comments submitted by EEI)
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	

10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-004-X
Poll Period:	10/8/2014 - 10/17/2014
Total # Opinions:	314
Total Ballot Pool:	374
Summary Results:	83.96% of those who registered to participate provided an opinion or an abstention; 96.63% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		

1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Abstain	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	

2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		

3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	

4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Abstain	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Negative	COMMENT RECEIVED
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	

5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	

5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	

6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-007-X
Poll Period:	10/8/2014 - 10/17/2014
Total # Opinions:	314
Total Ballot Pool:	374
Summary Results:	83.96% of those who registered to participate provided an opinion or an abstention; 96.63% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		

1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Abstain	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	

2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		

3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	

4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Abstain	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Negative	COMMENT RECEIVED
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	

5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	

5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	

6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-010-X
Poll Period:	10/8/2014 - 10/17/2014
Total # Opinions:	315
Total Ballot Pool:	374
Summary Results:	84.22% of those who registered to participate provided an opinion or an abstention; 95.52% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		

1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Abstain	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	

1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	

2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	

3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	

3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Abstain	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	

5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	

6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		

9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-010-2
Poll Period:	10/8/2014 - 10/17/2014
Total # Opinions:	316
Total Ballot Pool:	374
Summary Results:	84.49% of those who registered to participate provided an opinion or an abstention; 85.93% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	

1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Abstain	
1	FirstEnergy Corp.	William J Smith	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Negative	COMMENT RECEIVED
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	COMMENT RECEIVED
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	COMMENT RECEIVED
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by Nebraska

				Public Power District)
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe Obrien NIPSCO)
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	COMMENT RECEIVED
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		

1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	COMMENT RECEIVED
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	

3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Negative	COMMENT RECEIVED
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MidAmerican Energy Company)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Negative	COMMENT RECEIVED
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (Joe O'Brien)

3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	

4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Candace Morakinyo Wisconsin Electric)
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	

5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	EDP Renewables North America LLC	Heather Bowden		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FirstEnergys comments)
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC comments)
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support Joe O'Brien's comments on behalf of Jerry Freese.)
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	

5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI's Comments)
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	COMMENT RECEIVED
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	

6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support FirstEnergy Comments)
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Negative	SUPPORTS THIRD PARTY COMMENTS - (NYPA and NPCC)
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	COMMENT RECEIVED
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	

6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2014-02 CIP-011-X
Poll Period:	10/8/2014 - 10/17/2014
Total # Opinions:	315
Total Ballot Pool:	374
Summary Results:	84.22% of those who registered to participate provided an opinion or an abstention; 98.13% of those who provided an opinion indicated support for the VRFs and VSLs

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	NERC Notes
	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		

1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Abstain	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Abstain	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman		
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Jamison Cawley	Abstain	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple		
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Abstain	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA's)

1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	

2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach		
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	

3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	COMMENT RECEIVED
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist		
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	

4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Abstain	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Negative	COMMENT RECEIVED
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Abstain	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	

5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	EDP Renewables North America LLC	Heather Bowden		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Abstain	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPPD)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		

5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri		
6	AEP Marketing	Edward P. Cox	Abstain	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	

6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S Parsons	Abstain	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Individual or group. (70 Responses)
Name (51 Responses)
Organization (51 Responses)
Group Name (19 Responses)
Lead Contact (19 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (15 Responses)
Entity's Name: (70 Responses)
Question 1 (51 Responses)
Question 1 Comments (55 Responses)
Question 2 (48 Responses)
Question 2 Comments (56 Responses)
Question 3 (50 Responses)
Question 3 Comments (56 Responses)
Question 4 (48 Responses)
Question 4 Comments (56 Responses)
Question 5 (47 Responses)
Question 5 Comments (56 Responses)
Question 6 (50 Responses)
Question 6 Comments (56 Responses)
Question 7 (46 Responses)
Question 7 Comments (56 Responses)

Group
Tennessee Valley Authority
Brian Millard
No
1. CIP-003-6 R2 - The Registered Entity (RE) appreciates the work of the SDT; however, the RE objects to the requirement in CIP-003-6 to develop cyber security plans for Low Impact assets. Creation of cyber security plans for Low Impact assets adds nothing in terms of increased reliability and should therefore be eliminated. The SDT should consider incorporating the policy requirements applicable to Low Impact assets into the appropriate existing standards. Any requirements associated with cyber security awareness for Low Impact systems should be written into CIP-004. Any physical access control requirements for Low Impact systems should be written into CIP-006. Any electronic access control requirements for Low Impact systems should be written in CIP-005. Any Cyber Security Incident Response requirements for Low Impact systems should be incorporated into CIP-008. Moving the required policy into the appropriate standard more effectively addresses the directive to address Low Impact assets. Placing security controls for remote access, physical security, incident response, and cyber security awareness into a standard governing security management is both confusing and

inconsistent with the existing standards framework. 2. CIP-003-6 R2 VSL - The SDT should consider the VSL associated with CIP-003 R1 and R2 in context. Failure to document or implement a security plan for a Low Impact system inherently poses less risk than for Medium or High Impact systems, yet the VSL rating for both is Severe. The VSL for Low Impact systems should be lower than for High or Medium Impact systems. 3. CIP-003-6 Attachment 1 - The requirements in the security plan belong in the requirements section of the standard, not as an attachment, as noted in comment #1 above. Element 2 addresses physical access controls for the Low Impact BES Cyber System Electronic Access Point (LEAP). LEAPs are not required to be established until September 1, 2018 per Element 3. As written, however, the requirement to physically protect LEAPs would begin five months before they are established. Element 3.1 , Electronic Access Controls states: “For any Low Impact External Routable Connectivity, establish a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all other access.” The RE is concerned that without specific language to clarify or limit the applicable scope, the establishment of a LEAP would assume the establishment of an ESP, which may inappropriately subject those systems to CIP-005-6 R1. Similarly, establishing controls to permit “only necessary inbound and outbound access and denies all other access” may inappropriately bring CIP-007-6 R1 in to scope. Attachment 2 of Element 3 states that documentation may include “inbound and outbound connections (e.g. IP addresses, ports, services) for any Low Impact BES Cyber System Electronic Access Point are confined to only those the Responsible Entity deems necessary”. This is essentially a restatement of the “Measures” in CIP-007-X R1, which implies this requirement is in scope as well. The RE suggests the SDT revise the Attachment 1 and Attachment 2 language to clearly delineate the respective scope for Low Impact systems versus Medium and High Impact systems. 4. CIP-003-6 Attachment 2 - Attachment 2 does not offer much clarity beyond what is already documented in Attachment 1. The RE suggests that example evidence be documented in a table format similar to that used in CIP-004 -CIP-011 and provide supplemental guidance regarding the type(s) of evidence that would document compliance with the standard. 5. CIP-003-6 Guidelines and Technical basis - The guidance for R2 states “Using the list of assets from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the protections of all low impact BES Cyber Systems.” This guidance is in direct contradiction with CIP-002-5 R1.3 which states a discrete list of Low Impact BES Cyber Systems is not required. The SDT should consider whether a Low Impact system list should be generated as a result of the requirements in CIP-002-5, or revise the guidance in CIP-003-6 R2 to remove language that is contingent upon a Low Impact system list.
No
1. Low Impact External Routable Connectivity (LERC) Definition - Because LERC is communication between Low Impact BES Cyber Systems and Cyber Assets outside the asset, it would not include communication that is routed through a non-BES Cyber Asset such as a historian or jump host located in a DMZ. In those cases, a BES Cyber System would not be communicating outside the asset. The RE suggests the SDT clarify that the intent is to exclude this type of communication. 2. Low Impact BES Cyber System Electronic Access Point (LEAP)

Definition - The term “allows” in the definition is too broad and could inappropriately include assets such as switches, hubs, or other transport devices. The RE suggests using the term “controls” or “restricts” instead.
No
1. Guidelines and Technical Basis - Requirement 4 Attachment 1 Removable Media Page 43 states the following: “Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.” The statement that “…user(s) must have authorized electronic access to the applicable system…” is not a CIP requirement and should not be included in the Guidelines and Technical Basis section of the document. Additionally, it is not necessary that a user of an authorized removable media device have electronic access to the applicable system. An individual with physical access to a system could be connecting removable media for someone with electronic access but working remotely. 2. CIP-010-6 R4 and Attachment 1 - The required elements and R4 refer to “documented plan(s) for Transient Cyber Assets and Removable Media”. Neither requirement 4, the three pages of Attachment 1 “Required Elements for Plans”, Attachment 2, nor the CIP-010-2 Definitions include a clear definition for what constitutes a “plan”. Certain sections indicate that policies could suffice, but in other sections it only requires “documentation” and seems to purposefully leave out “policies”. The language as written may intend to allow entities flexibility for how a “plan” is documented, but may have the unintended consequence of deferring to the judgment of the auditor to determine what level of “documentation” constitutes a “plan”. The RE suggests the SDT clarify the requirement that a ”plan” can be any type of documentation defined by the RE that meets the “Required Elements for Plans for Transient Cyber Assets and Removable Media” in Attachment 1.
Yes
Yes
Yes
No
Group
Northeast Power Coordinating Council
Guy Zito
No
Request clarification on where the dividing line is between Element 4 (Cyber Security Incident Response) and EOP-004. The Element references in Attachment 2 should match the Elements in Attachment 1, otherwise industry could draw incorrect conclusions. Recommend adding

“As needed” to the beginning of Attachment 1 4.7 because not every incident/test needs an updated Incident Response Plan.
No
Recommend removal of “and controls” from the Technical Guidance on Low Impact Cyber System Electronic Access Point (LEAP) to be consistent with the Definition of LEAP. Currently, the LEAP Technical Guidance says “is the interface on a Cyber Asset that allows and controls the LERC,” while the LEAP Definition says “A Cyber Asset interface that allows the Low Impact External Routable Connectivity.”
No
For clarity, suggest revising Attachment 1 2.1 from “each Responsible Entity shall use one or a combination of the following methods: ” to “each Responsible Entity shall use at least one or a combination of the following methods: ” For clarity, suggest revising Attachment 1 2.2 from “each Responsible Entity shall use one or a combination of the following methods:” to “each Responsible Entity shall use at least one or a combination of the following methods:” As written, Attachment 2.3 requires each Entity to review each vendor’s policies/procedures. This may be too burdensome for the industry. Suggest a different solution is needed. Recommend changing from “Responsible Entities shall determine whether additional mitigation actions are necessary ” to “Responsible Entities may determine whether additional mitigation actions are necessary ” Attachment 1 1.2 covers Transient Cyber Asset authorization, however there is no corresponding part for vendor/contractor authorization. Suggest adding a part for Responsible Entity authorization of vendor/contractor use of Transient Cyber Assets.
No
Based on the new definitions, it is unclear on whether a cyber asset can be classified as multiple asset types and would therefore be subject to multiple levels of requirements, i.e. a BES Cyber Asset or a Protected Cyber Asset can also be a Transient Cyber Asset. If a BES Cyber Asset or a PCA also meets the definition of Transient Cyber Asset, there is nothing in the language that says one classification supersedes or precludes another. Solely based on the definitions, it would appear that an entity would have to classify an asset by all the definitions that apply. Recommendations: • Add the following sentence to definition of Transient Cyber Asset: "A Cyber Asset that meets the definition of BES Cyber Asset shall not be considered a Transient Cyber Asset." • Add a minimum requirement to the PCA definition. “If a PCA is connected for less than 30 days then it is a TCA and more than 30 days it is a PCA.”
Yes
Yes
Yes
To avoid industry confusion, recommend changing “elements” to another label such as “plan elements” or “items.” Recommend quality assurance review before future postings, to avoid reviewers’ confusion or need to decipher how to connect related information.

Group
Colroado Springs Utilities
Shannon Fair
Agree
CSU agrees with the changes to CIP-003-6, R2 including the use of Attachment. CSU recommends the following edit to Attachment 1: “Each Responsible Entity shall reinforce, at least once every 15 calendar months” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle.
Yes
CSU supports the new definitions for Low Impact External Routable Connectivity and Low Impact BES Cyber Systems Electronic Access Point.
Yes
CSU agrees and supports the changes that were made to CIP-010-2, R4.
Yes
CSU agrees with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. Since “Media” is itself not a defined term, CSU recommends either defining “Media” or not capitalizing the term.
Yes
CSU agrees and supports the proposed implementation plan deadlines for CIP-003-6, R2.
Yes
CSU supports the removal of the IAC language from the 17 requirements based on the FERC directive.
No
Individual
Steve Hamburg
Encari
Yes
No
The LERC definition requires clarification as to the external connectivity that is the focus of the definition. Suggest that "outside the network" replace "outside the asset." The definition should read: Low Impact External Routable Connectivity (LERC): Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the network containing those low impact BES Cyber System(s). Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Yes
No
It remains unclear as to whether a Transient Cyber Asset can also be considered as a BES Cyber Asset. If the intent is to exclude Transient Cyber Assets from the classification of BES Cyber Assets, the definition of Transient Cyber Asset should expressly state, "Transient Cyber Asset: A Cyber Asset, (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Cyber Asset meeting the definition of a Transient Cyber Asset may be excluded from classification as a BES Cyber Asset."
Yes
Yes
Yes
The definition of BES Cyber Asset has been modified to remove the exclusion of Transient Cyber Assets. This creates confusion as to whether a Transient Cyber Asset may still be considered a BES Cyber Asset since the definition of Transient Cyber Asset does not indicate whether a Transient Cyber Asset may be excluded from the classification of a BES Cyber Asset.
Individual
Alshare Hughes
Luminant Generation Company, LLC
Yes
We recommend the revisions below to improve or clarify the current draft language. 1) Attachment 1, Element 2 – Recommend removal of “Based on need” qualifier that renders requirement to “restrict physical access” more stringent that comparable requirement for Medium Impact BES Cyber Systems without External Routable Connectivity (CIP-006 R1.1). Also recommend removal of “based on need” language in corresponding Attachment 2, Element 2, Item 2. 2) Attachment 2, Element 4 – The requirements include identification, classification and response in 4.1 and incident handling in 4.4. There appears to be an overlap and redundancy with these terms. Recommend revision to 4.1 to “Identification and response to …”. 3) Attachment 1, Element 4.7 – The current language unconditionally mandates the updating of the incident response plan regardless of need. Recommend revision to: "Updating the Cyber Security Incident response plan, if necessary as determined by the Responsible Entity, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident. If no updates are deemed necessary, this decision should be recorded within 180 days." Also recommend revision of language in

corresponding Attachment 2, Element 4, last paragraph. 4) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – The last sentence discussing LERC is not clear. Recommend revision to The SDT intends that IED to IED communications be exempt from any requirement to use an electronic access point, even if there is Low Impact External Routable Connectivity. Through this exemption, the SDT intends to not preclude the use of time-sensitive reliability enhancing data exchanges." 5) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – In language describing LEAP, recommend replacing "internal interface" with "an interface" and dropping the "facing the low impact BES Cyber System" language. Well-intentioned but may confuse implementers 6) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – Sentence "However the LERC between assets,… must also pass through the single LEAP" should be revised to say, "…must also pass through a LEAP." 7) Guidelines and Technical Basis, Discussion of R2, Attachment 1, LEAP discussion – Delete "physically" from "unidirectional gateway that physically enforces outbound-only data flows". Change "LEAP are not to be considered EACMS…" to "A LEAP is not to be considered an EACMS…". Change "However they are required" to "However it is required". Delete last sentence ("It is also not the intent of the SDT…" or change to: "A LEAP is not required for any BES Asset where there are low impact BES Cyber Systems but no LERC". 8) Guidelines and Technical Basis, Discussion of R2, Attachment 1, Electronic Access Controls discussion – Within the first main section on page 34 beginning with "The electronic access controls…", recommend replacing "shall" with "should" in the second sentence. This would be more appropriate language for guidance. 9) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – in the diagram for Reference Model 2, change "an LEAP" to "a LEAP". 10) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – Cyber Security Incident Response, first paragraph – "For assets that do not have LERC…" raises the question of whether the assets that do have LERC should have "real time monitoring." There is no monitoring requirement in R2 so this sentence should be deleted. 11) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – Cyber Security Incident Response, second paragraph – per previous comments update to plan(s) within 180 days of a test or an actual incident should only be required if the Responsible Entity determines revisions to the plan are necessary.

Yes

Yes

We recommend the revisions below to improve or clarify the current draft language. 1) Attachment 1, Element 1.3 – "Live operating system and software executable only from read-only media" is not sufficiently clear. Suggested revision: "Use of operating system software and other required executables installed from read-only media." 2) Attachment 1, Element 1.4 – Suggest revision of element title to "Malicious code prevention or mitigation" AND begin first sentence with "To prevent or, if necessary, mitigate the introduction of malicious code,…" 3) Attachment 1, Element 1.5 – Suggested revision of element title to "Unauthorized use prevention or mitigation" AND begin first sentence with "To prevent or, if necessary, mitigate the impact of unauthorized use,…" 4) Attachment 1, Element 2.2 – Suggested revision of "…live operating system and software executable only from read-only media" to "…operating system software and other required executables installed from read-only media"

to add clarity. 5) Attachment 2, Evidence for Element 1.3, 1.4, 1.5, 2.1, 2.2 – Suggest deletion of last sentence in each of these statements as the current language introduces a loophole. The requirements in Attachment 1 are written to provide flexibility to "do A, or B, or C, or something else to mitigate risks" so there should be no circumstance under which an entity can assert it is not possible to do anything to mitigate the security risks. 6) Guidelines and Technical Basis, Discussion of Element 1.4 and 3.2 – The last sentence should be deleted. The statement "Entities should also consider whether the detected malicious code is a Cyber Security Incident" suggests a requirement that is not included in any "R" statement in the draft language. 7) Guidelines and Technical Basis, Discussion of Element 1.5, first bullet – Suggested revision of "…Physical Security Perimeter or other physical location that manages unauthorized physical access…" to "…Physical Security Perimeter or other physical location that manages physical access…". 8) Guidelines and Technical Basis, Discussion of Element 1.5, second bullet – Disk encryption will not protect a Transient Cyber Asset from unauthorized physical access. Suggested revision: "Full disk encryption with authentication is an option that can be used to mitigate the risks associated with unauthorized physical access to a Transient Cyber Asset."
Yes
Yes
Yes
Individual
Thomas Haire
Rutherford EMC
No
No
No
No
Yes
No
The IAC language provided more proactive results based approach to truly identify, assess, and correct problems rather than follow standards.

No
Individual
Dan Bamber
ATCO Electric
Yes
Yes
Yes
No
ATCO Electric Transmission requests further clarification on the Removable Media definition. In the scenario where a USB stick (removable media) is connected to a laptop (transient cyber asset) would these two items, together, be considered removable media or a transient device?
Yes
Yes
No
Individual
Dan Roethemeyer
Dynegy
No
For physical access controls, the draft reads that physical access be restricted 2 ways (1) the asset or location..... and (2) the Low EAP. I don't understand why it has to be both. Suggest changing the "and" to an "or". Also, if (2) is required, that would seemingly require an asset inventory list which is not required for Low impact assets.

Individual
Heather Laws
PNM Resources, Inc
Agree
EEI
Individual
Mike Marshall
Idaho Power
No
The main issue is with section 3 of Attachment 1. There has been no good explanation given for how this requirement will be audited without providing a list of Low Impact BES Cyber Systems which contradicts the wording of CIP-002. Additionally, the “Rationale for Requirement R2” states that "there continues to be no compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems." Yet the entities are to identify (without maintaining a list) all of the Low Impact Cyber Systems that require these electronic access controls. It seems that the v5 standards need to settle into some level of stability and then address further security concerns such as the ones addressed in section 3 of the Attachment 1 in a later version or at the very least revise the wording to be more clear with what will be required, how it will be approached, and how it will not be in conflict with other CIP standards.
Yes
Yes
Yes
No
The time frames still do not provide enough time for entities to adjust to and increase of scope of this magnitude.
Yes
No
Individual
Debra Horvath
Portland General Electric
Agree
Edison Electric Institute

Individual
John Brockhan
CenterPoint Energy Houston Electric LLC.
No
Attachment 1, Element 4.7 - CenterPoint Energy agrees with EEI's comment. Element 4.7 implies that the Cyber Security Incident response plan should be updated within 180 calendar days after completion of a Cyber Security Incident response plan(s) or actual Reportable Cyber Security Incident. However, this may not always be the case. CenterPoint Energy recommends adding the words ", if needed" after "180 calendar days."
No
CenterPoint Energy generally agrees with requirement R4 and the documentation of a plan to address Transient Cyber Assets and Removable Media. As written in the Guidelines and Technical Basis for R4 Attachment 1, Elements 2.1, 2.2, and 2.3, the requirement allows entities the ability to review the assets to the best of their capability and meet their obligations. Additionally, entities are to document and implement their procedures to mitigate security vulnerabilities and malicious code. In Attachment 1 under Element 2.3, CenterPoint Energy believes that the Responsible Entity should determine the frequency of mitigation actions for Transient Cyber Assets owned or managed by vendors or contractors as noted in the documented plan required in R4. As it is currently written, it can be interpreted as requiring Responsible Entities to perform mitigation methods stated in Elements 2.1, 2.2, and 2.3 each time the vendor or contractor-owned device is connected to a BES Cyber System. This would be operationally inefficient if the vendor is connecting to multiple BES Cyber Systems consecutively within the trusted environment. For example, if a vendor is updating firmware at multiple substations, the Responsible Entity may scan/review the vendor-owned Transient Cyber Asset for security patches and antivirus once, prior to connecting to the first BES Cyber System. The review would be valid and effective for the duration of the firmware update at multiple substations as long as the Transient Cyber Asset is not connected to an unsafe/untrusted environment and is used within the protected environment. CenterPoint Energy recommends adding clarification to the Guidelines and Technical Basis under "Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors" for Elements 2.1, 2.2, and 2.3. CenterPoint Energy suggests the following wording to be added to Elements 2.1, 2.2, and 2.3, "prior to connecting their devices to the applicable systems within the trusted environment." Attachment 1, Element 3.2 - CenterPoint Energy agrees with EEI's comment. This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 does not allow for these options. Also, Element 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. CenterPoint Energy recommends changing "scan Removable Media outside of the BES Cyber System" to "use a method to scan

Removable Media for malicious code and a procedure to respond to detected malicious code.”
Yes
Yes
Yes
CenterPoint Energy supports this revision approach for IAC. As proposed by NERC, the Company looks forward to the concepts of IAC being implemented within the final framework of the Reliability Assurance Initiative (RAI).
Individual
Jo-Anne Ross
Manitoba Hydro
Yes
Yes
Yes
Yes
Yes
Yes
No
Group
Dominion
Greg Dodson
No
1. The R2 Attachment 1 Element 2 and Attachment 2 Element 2 Part 2 that describe authorization “based on need” for physical security controls is problematic and should be removed. The concept appears to be the same as used in CIP-004 R4.1 where you should have some justification of the business need for authorization of electronic and unescorted physical

access and access to BES Cyber System Information, the SDT used it in a different context in CIP-003-6. However, the guidance states, “The requirement does not imply that a specific business need must be documented for each access or authorization of a user for access. The SDT intent is that this need at the higher level be documented such that the requirement cannot be interpreted to mean that any and all access must be restricted. The requirement does not imply that a specific business need must be documented for each access or authorization of a user for access.” A policy level document that requires no action is merely an administrative burden that doesn’t meet the minimum elements of a properly developed Standard. The clause “based on need as determined by the Responsible Entity” should be removed from [Element] 2. Physical access controls in CIP-003-6 – Attachment 1, and item 2 of Element 2 in CIP-003-6 – Attachment 2 should also be removed. 2. The guidance associated with R2 (page 31 of 37 in the clean version) states, “The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed.” This guidance is should be reworded for clarity as follows: “The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they dostill meet the definition of having a 15-minute adverse impact so some protections are needed.” As stated, the wording creates confusion between “low impact” and “no impact”. 3. The guidance associated with R2 Attachment 1 (page 33 of 37 in the clean version) states “Low Impact BES Cyber System Electronic Access Point (LEAP) – is the interface on a Cyber Asset that allows and controls the LERC.” This language doesn’t match the definition. The sentence should be changed to, “Low Impact BES Cyber System Electronic Access Point (LEAP) – A Cyber Asset interface that allows Low Impact External Routable Connectivity.” 4. Element references in Attachment 2 should match the Elements in Attachment 1, otherwise industry could draw incorrect conclusions. 5. By not placing like requirements throughout the standards, there’s an opportunity to violate more than one requirement. For example, with Cyber Security Awareness and Incident Response, if a facility has all impact levels and a Cyber Security Incident occurs, there’s the potential to violate both CIP-008-5 and CIP-003-6. 6. Requirement [part, element] 4.7 in CIP-003-6 – Attachment 1 assumes that the incident response plan will require an update, which may be an incorrect assumption. The phrase, “as required” should be appended to 4.7. 7. CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation: Change Subpart 1.2.2 to “Physical access controls.” 8. CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation: Add “, if needed,” after “180 calendar days.” 9. CIP-003-6 Attachment 2 and Guidelines and Technical Basis for element 2: Attachment 2 (examples of evidence) for element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for element 2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation: Include “perimeter controls” under element 2, Attachment 2 in the example: “(e.g., card key, special locks, perimeter controls).
No

1. In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation: Clarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to allow for point-to-point communications (e.g., over fiber) to use routable communication protocols for time sensitive protection and/or control functions.
No
1. For clarity, suggest changing 2.1 from “each Responsible Entity shall use one or a combination of the following methods:” to “each Responsible Entity shall use at least one or a combination of the following methods:” 2. For clarity, suggest changing 2.2 from “each Responsible Entity shall use one or a combination of the following methods:” to “each Responsible Entity shall use at least one or a combination of the following methods:” The phrase “(per Transient Cyber Asset capability)” should be added to 1.5 and 2.2 as is insinuated in the guidance (“If a Transient Cyber Asset is unable to perform…”). 3. CIP-010-2 Attachment 1: The use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is unnecessary and implies a second step such as approval of who can use the TCA, where, and how, which is unclear – the plan should identify the users, locations, and uses of the TCA. Recommendation: Remove “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. 4. CIP-010-2 Requirement R4 ends with “include the elements in Attachment 1”, although the first sentence in Element 1 says “include each of the element provided below” the actual “elements” are not labeled “elements” as in Attachment 2, which references the elements in Attachment 1. Recommendation: Add “Element” before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses.
Yes
Yes
Yes
No
Individual
Joe O'Brien on behalf of Jerry Freese
NIPSCO
These commments are copied from an EEI Draft which we support. If EEI has submitted comments than these may be redundant. Thanks
No
Comment 1.1: CIP-003-6 Rationale for Requirement R2: “Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised.” Aggregating low impact BES Cyber Systems across multiple assets does not reflect a true risk-based assessment and therefore this sentence is

not accurate. Recommendation: Delete this sentence. Focuses on Rationale, not requirement Comment 1.2: CIP-003-6 – Attachment 1: The language in Element 1 “using one or a combination of the following” is inconsistent with the Element 2 language “through one or more of the following.” Recommendation: Change the language in Element 1 to “through one or more of the following.” Minor wording issue Comment 1.3: CIP-003-6 – Attachment 1: CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation: Change Attachment 1, Element 2 to “Physical security controls” to be consistent with the language of the standard. Please edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs) to CIP-003-6 R1 are consistent. Comment 1.4: CIP-003-6 Requirement R2 ends with “include the elements in Attachment 1”, although the first sentence in Element 1 says “include each of the elements provided below” the actual “elements” are not labelled “elements” as in Attachment 2, which references the elements in Attachment 1. Minor format issue. Recommendation: Add “Element” before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses. This would also be helpful for Attachment 1 in CIP-010-2. Comment 1.5: The “(LERC)” and “(LEAP)” acronyms are missing in Element 2, 3, and 3.1, which makes it harder to identify the use defined phrases in these elements. Recommendation: Add the “(LERC)” and “(LEAP)” to elements 2, 3, and 3.1 to make it easier to identify the acronym. Minor format issue Comment 1.6: CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation: Add “, if needed,” after “180 calendar days.” Point of clarification; valid Comment 1.7: CIP-003-6 Attachment 2 and Guidelines and Technical Basis for Element 2: Attachment 2 (examples of evidence) for Element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for Element 2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation: Include “perimeter controls” under Element 2, Attachment 2 in the example: “(e.g., card key, special locks, perimeter controls). Valid inconsistencies; Comment 1.8: CIP-003-6 Guidelines and Technical Basis, Requirement R2 Attachment 1 bold text subtitles on page 32: The subtitles are inconsistent with the element language in Attachment 1. Recommendation: Change the subtitle language to “Requirement R2 Attachment 1 – Cyber Security Awareness” and “Requirement R2 Attachment 1 – Physical Security Controls” (see Comment 1.2 above). Valid point of clarification

No

Comment 2.1: Use of “allows” in the LEAP definition does not allow for the use of an unmanaged hub. An unmanaged hub, which does not support access controls and may be merely acting as a central connecting point, could be considered an interface that “allows” Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs. Recommendation: Change “allows” to “controls” to allow for the use of unmanaged hubs as appropriate. Please also make sure this is changed in the Guidelines and Technical Basis and anywhere else the LEAP

definition is provided. Valid definition modification Comment 2.2: Because the acronyms LEAP and LERC are used to help simplify the terms defined and used in the standard, it would help to include the acronyms each time the terms are spelled out in full in the definitions and in the standards and related guidance. Recommendation: Insert the acronyms “(LERC)” and “(LEAP)” as they are spelled out in the definitions. Minor format issue Comment 2.3: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation: Change the exclusion sentence to: “Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).” Alternatively, Cclarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to include point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions. Valid point of clarification Comment 2.4: The definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation: In the Guidelines and Technical Basis for CIP-003-6, where LEAP is described, move the sentence “LEAP are not to be considered EACMS…” to create a second paragraph and add “However a LEAP can be implement within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself.” Valid point of clarification Comment 2.5: LERC definition or CIP-003-6 Guidelines and Technical Basis for Requirement R2 Attachment 1 – Electronic Access Controls: The following scenario is unclear: {Low impact BES Cyber System (e.g., control system) ---- |1| ---- Cyber Asset (e.g., data historian) ---- |2|} ---- Location X Where: {} represents the asset/site boundary, |1| represents a firewall or electronic access point (in this case firewall 1), and ---- represents a bi-directional routable communication Based on the language of the definition and CIP-003-6 it is unclear whether there is a LERC and LEAP in this scenario and if there is LERC, which firewall is the LEAP. The Guidelines and Technical Basis for CIP-003-6 say “the electronic access controls should address the risk of using the asset’s LERC to gain access to the low impact BES Cyber Systems.” However, this scenario would require an adversary to gain access to not one but of two access points, – the firewalls on either side of the Cyber Asset (firewall 2 and then firewall 1) to get access to the low impact BES Cyber System. Whereas, the examples provided all show one access point, the LEAP, which requires controls. Recommendation: Add this scenario to the CIP-003-6 Guidelines and Technical Basis, Responsible Entity to have the flexibility choose the LEAP, either firewall 1 or firewall 2. Valid point of clarification
No
Comment 3.1: CIP-010-2 R4: The placement of “under CIP Exceptional Circumstances,” is awkward. Recommendation: Move “under CIP Exceptional Circumstances” up in the

sentence, such that it reads "…shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s)…" Minor format issue Comment 3.2: CIP-010-2 Attachment 1: The use of "Authorized" in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and 2 it is implied by the language of 1.2 and 1.3. The language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization for the Transient Cyber Asset. The redundancy creates uncertainty in the interpretation of the standard. It could be interpreted to imply a second step in addition to the R4 plan. In other words, in addition to the R4 plan for Transient Cyber Assets and Removable Media, which includes the 1.2 and 3.1 authorization elements, the Responsible Entity must also have a separate, formal approval process plan to identify authorized users, authorized locations, and authorized uses for Transient Cyber Assets and a separate formal approval process to identify who is authorized to use and where they are authorized to use Removable Media. We believe the intent of the Standards Drafting Team is that the plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address thesee authorization elements. This flexibility will allow the Responsible Entity to either write a plan that specifically defines who is authorized to use the Transient Cyber Asset(s) for which uses and locations or include a separate authorization process, which may include a formal approval process, in the plan that identifies the users, locations, and uses authorized for the Transient Cyber Asset(s). It will also give the Responsible Entity the same flexibility for Removable Media authorizations. This flexibility is particularly needed for Responsible Entities that rely on contractor use of Responsible Entity managed Transient Cyber Assets and Removable Media who have less control over the contractor, i.e., the control is defined by a service agreement or contract. Giving the Responsible Entity flexibility on how to define the authorization process will allow them to align these requirements with their vendor contracts. Recommendation: Remove "Authorized" from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. Alternatively, clarify in the Guidelines and Technical Basis under Element 1.2 and 3.1 that the use of "Authorized" in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 does not require a formal approval process for each user, location, and use of the Transient Cyber Asset (or Removable Media), but gives the Responsible Entity the flexibility to develop an authorization plan that either directly defines authorization or requires a specific authorization process. This allows Responsible Entities to align their Transient Cyber Asset and Removable Media authorizations with their vendor contracts for use of Responsible Entity managed Transient Cyber Assets. Valid point of clarification Comment 3.3: CIP-010-2- Attachment 1 Elements 1 and 2 are grouped by whether a Transient Cyber Asset is owned or managed by the Responsible Entity or by a vendor or contractor. The intent of this grouping is good because it considers the level of control by the Responsible Entity. However, the actual groupings could result in a Transient Cyber Asset that falls under both element 1 and 2. For example, if a Responsible Entity owns the Transient Cyber Asset, but a contractor manages its use under a service management contract. Another scenario is that the vendor owns the Transient Cyber Asset, but the Responsible Entity manages it. For

these scenarios, it is unclear whether the Responsible Entity should include element 1 or 2 or both elements in their R4 plan(s). Recommendation: Remove “Owned or” from elements 1 and 2. Comment 3.4: CIP-010-2 - Attachment 1, Element 2.3: “Responsible Entities shall determine whether additional mitigation actions are necessary…” requires a statement that says no additional mitigation measures were identified as necessary, which creates an unnecessary administrative burden. Also, Element 2.3 is an element that should be addressed by the R4 plan for Transient Cyber Assets and Removable Media, the way Element 2.3 is written makes it look like a requirement rather than a plan element, which also causes confusion as to the frequency of review for elements 2.1 and 2.2. Element 2.3 as written suggests that a Responsible Entity must use the 2.3 and 2.4 mitigation methods prior to each connection of a vendor-owned Transient Cyber Asset in order to determine whether additional mitigation measures will be needed. This can be overly burdensome and unnecessary when a vendor is moving from system to system in a single day. Also, a Transient Cyber Asset may be owned by the Responsible Entity and managed by a vendor or owned by the vendor/contractor and managed by the Responsible Entity. The use of “vendor- or contractor-owned” in 2.3 is not consistent with these scenarios (see comment 3.3 above).We recommend restructuring Element 2.3 to make it clear that this – determining whether additional mitigations are needed before the vendor-owned Transient Cyber Asset is connected – is an element of the plan that should be addressed to manage the associated risk and not that elements 2.1, 2.2, and 2.3 need to be used prior to each connection. Recommendation: Change Element 2.3 to:Add “necessary” before “such actions.” Also, clarify in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how to manage vulnerability and malicious code reviews of their vendors or contractors and require additional mitigation actions. For example, one entity may require a vendor to plug a Transient Cyber Asset into a kiosk to scan for vulnerabilities and malicious code before each connection. However, this approach may not be feasible for all entities, so defining a process to initially and periodically check and audit vendor/contractor processes for vulnerability and malicious code mitigation. Specifically, “prior to connecting the vendor- or contactor-owned Transient Cyber Asset” does not require that 2.1, 2.2, and 2.3 before each connection, but that the Responsible Entity should define a process to manage the use of vendor- or contractor- managed Transient Cyber Assets to mitigate vulnerabilities and malicious code. Also, change “owned” in 2.3 to “managed.” Comment 3.5: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped. Recommendation: Make it clear in the Guidelines and Technical Basis that “mitigate” and “mitigation” does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system that the Transient Cyber Asset or Removabl ???e Media is used on. Also, it may be impossible to detect every piece of malicious code. Mitigation is meant to reduce security risks, but elimination of all risk is impossible. Comment 3.6: CIP-010-2 – Attachment 2, Element 3.2: This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the

Responsible Entity to take any action other than scanning Removable Media at some point in time. Recommendation: Change “scan Removable Media outside of the BES Cyber System” to “use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code.” Comment 3.7: CIP-010-2 – Attachment 2, Element 1.2: The second sentence under Element 1.2 is a restatement of Attachment 1, Element 1.2 and is not an example of evidence. Recommendation: Remove the second sentence under Attachment 2, Element 1.2: “The documentation must…” to keep the text in Attachment 2 focused on examples of evidence and not include requirements. Comment 3.8: Guidelines and Technical Basis for R4, Attachment 1, Element 1.1: inventories of Transient Cyber Assets is allowed by individual or group – individually or by asset type, therefore language under Element 1.1 should be consistent, allowing inventory of devices or device type. Recommendation: Add “or device types” to the second sentence: “pre-authorize and inventory of devices or device types or authorize devices or device types at the time of connection or use a combination of these methods.”
No
Comment 4.1: Transient Cyber Asset Definition: The “and” in the parenthesis after “A Cyber Asset,” is confusing. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. Also, the parenthetical for the examples is misplaced; it refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, “directly connected” may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Recommendation: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.” Also, if the intent is for the Transient Cyber Asset definition to apply to both routable and non-routable communications, clarify this in the Guidelines and Technical Basis for CIP-010-2.
No
Comment 5.1: CIP-003-6, Attachment 1, Element 2 compliance date of April 1, 2018: According to the Implementation Plan, the Element 2 physical access controls must be applied to LEAPs by April 1, 2018; however, the LEAPs are not identified under Element 3, which must be applied by until September 1, 2018. Recommendation: Change the compliance date for Element 2 to September 1, 2018 to allow time for the LEAPs to be identified under Element 3 and the physical access controls to be applied to them under Element 2. Alternatively, leave the compliance date for physical access controls to “the asset or the locations of the low

impact BES Cyber Systems within the asset" as April 1, 2018 and change the compliance date for requiring physical access controls to the LEAPs to September 1, 2018.
No
Comment 6.1: CIP-011-2 R1/CIP-011-X: Information protection item CIP-003-4, R4.3 allowed for annual assessment of adherence to the BES Cyber System information protection program and development of an action plan to remediate any identified deficiencies. This language provides a risk management approach: identifying the information that needs to be protected, implementing procedures to protect that information, and annually assessing adherence to that policy and incorporating lessons learned. Without the R4.3 language, any violation of the procedure will result in a Severe violation of the requirement and under the Violation Severity Level table for R1. Only a Severe level is listed for if plan is not documented or implemented, therefore if the plan is documented and partially implemented (i.e., deficiencies are found), then it is a Severe VSL. Recommendation: Add a part 1.3 to R1 to address this concern: "The Responsible Entity shall, at least annually, assess adherence to its procedures for protecting and securely handling BES Cyber System Information, including identification, protection, and handling; document the assessment results; and implement an action plan to remediate deficiencies identified during the assessment." Adjust the Violation Severity Level table for R1 accordingly. Also, change the language of the existing Severe VSL to tier possible violations into lower levels commensurate with the risk.
No
Individual
Leonard Kula
Independent Electricity System Operator
No
We disagree with the revised structure of CIP-003-6. The concept of using tables to articulate the requirements is effective in all other standards and should be equally effective in CIP-003-6. The proposed structure introduces inconsistency of structure which is confusing. Attachments should not be used to articulate requirements. Attachment 1 is a list of requirements and should be treated as such within the main body of the standard. Attachments should only be used for guidance or informational items, not requirements that must be complied with.
No
The definition for LERC states that "Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s)." We suggest that the statement should include both BES Cyber Systems and BES Cyber Assets as LERC should apply to both systems and assets and should read: Bi-directional routable communications between low impact BES Cyber Asset(s)/BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s)/BES Cyber Asset(s).

No
We disagree with the structure approach to address transient cyber assets in a separate requirement as it leads to inconsistent approaches between BES Cyber Systems/Assets and transient assets. We suggest that it would be much simpler and more efffective if transient assets were added to the Applicable Systems column where appropriate throughout the standards. It is not clear why R4 substantially deviates from the table format of the sub-requirements. If it is necessary to have a separate requirement for transient assets we recommend that R4 be revised to reflect the table format of the sub-requirements and not use an attachment. It is not appropriate to put sub-requirements in an attachment, they should reside in the main body of the document along with the requirement wording as is done for all other CIP standards.
No
The definition of Removable Media refers to media that are "capable of transmitting executable code to: ". We suggest that the word "transmitting" is incorrect and should read "transferring". Media such as floppy disks do not transmit but one can transfer executable code from the disk to another media.
Yes
Yes
No
Individual
Dave Francis for Terry Bilke
MISO
NO COMMENT
NO COMMENT
Yes
MISO supports the changes made by the SDT to Requirement R4 and Attachment 1. ATTACHMENT 1: The posted language for Attachment 1, Element 2.3 requires, “Responsible Entities shall determine whether additional mitigation measures are necessary…”, intending the entity make an affirmative decision to allow the device to connect. It is recommended revising as, “Responsible Entities shall determine whether any additional mitigation actions are necessary to clarify and entity may allow connection of the device without requiring modifications. GUIDELINES AND TECHNICAL BASIS: The posted language for the Transient Cyber Assets in Attachment 1, Element 1 allows for authorization to be done individually or by asset type; however the Guidelines and Technical Basis for Element 1 does not discuss the ability to authorize based on a group of assets. SMUD recommends language be added to allow “authorization individually or by groups of assets” to the Guidelines and Technical Basis for Element 1.1.

Yes
MISO supports the changes made by the SDT to these definitions.
Yes
MISO supports the changes made by the SDT to the implementation plan.
Yes
MISO supports the removal of the IAC language from the 17 requirements and the continued work by NERC to develop the Reliability Assurance Initiative.
No
Individual
Tony Eddleman
Nebraska Public Power District
No
Recommend the requirements for physical security of low assets be deleted. This requirement is repetitive of safety requirements in the National Electrical Safety Code (NESC), Section 11 - Protective arrangements in electric supply stations, paragraph 110 General requirements. The NESC includes requirements to protect the public from high voltages. The safety aspects of the NESC are more stringent than the requirements in the proposed NERC standard and public safety is a higher concern than the less likely occurrence of security concerns at a low impact asset. Specifically the proposed CIP-003-6 requires: Element 2: Examples of evidence for element 2 may include, but are not limited to: 1. Documentation of one or more access controls (e.g. card key, special locks), monitoring controls (e.g. alarm systems, human observation), or other operational, procedural or technical physical security controls to restrict physical access to both: a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and b. The Cyber Asset, if any, containing the Low Impact BES Cyber System Electronic Access Point. 2. Documentation showing that the physical access restrictions cited above are based on need, which may include, but is not limited to, a policy describing the high level operational or business need(s) for physical access. The proposed NERC requirement allows technical physical security controls to restrict physical access to both. A fence with a locked gate, which is required by the NESC appears to meet the proposed NERC requirement to restrict physical access to both the asset and the cyber asset. The other suggestions in the draft standard could be provided in a best practices document. The requirement for physical security of low assets should be deleted.
No
The LERC should specifically exclude communications aided relaying used for pilot relaying protection. Also, there is a high risk of confusion when using technical jargon in NERC definitions. Both of these definitions fall within this high level of confusion. If a national reliability standard requires too much technical jargon, it is written at the wrong level for its purpose. The reliability standard should be written to avoid the use of these definitions.
No

While the language in the proposed requirements is a good practice, it creates significant compliance burden for entities to maintain documentation to prove compliance; plus, additional resources will be required to implement compliance controls that yield minimal risk reduction for the reliability of the BES. Transient devices will be a source of possible violations in future internal compliance reviews for self reports and also compliance audits. Section 1.2 of Attachment 1 is not needed and should be removed. Requirements already exist for anyone having access to protected cyber systems. Section 1.2 puts an entity in double jeopardy of violating multiple requirements for one action. The same comments apply to section 3.1 of attachment 1 and this requirement should be removed.
No
As stated in previous comments, we do not support the removal of the IAC language. Removal of the IAC language is a return to zero tolerance and RAI does not magically make a violation disappear. Our suggestion is to delete any requirement from the standard that contains IAC language. This is our opportunity as an industry to remove the sections, develop better language as FERC allowed, or face multiple violations of these zero tolerance requirements for many years. We've rushed through all the previous versions to meet a deadline. This is the time to work on a solution and get a better standard. We are working to meet compliance deadlines for version five standards while making changes to the standards – this can't be a good practice. FERC approved the version five standards; they didn't remand them back. We have an official compliance date to meet for version five. Worse case, let's use the IAC language as currently approved.
Yes
The NERC CIP standards have resulted in numerous violations to registered entities and have been difficult to implement. These standards must get to a steady state and changes to the standards should be limited to an absolute minimum.
Group
Seattle City Light
Paul Haase
SMUD
No
Seattle City Light supports the proposed CIP v5 revisions, but remains concerned about the compliance aspects of providing protections for Low-rated systems and assets. Our primary concern is that in a multi-impact rated program (high, medium and low), any failure to fulfill a requirement such as Attachment 1, Element 1 Cyber Security Awareness or Element 4 Cyber Security Incident Response, could result in violation of CIP-003-6, R2, CIP-004-5, R1 and CIP-008-5, i.e. a single compliance failure could result in multiple violations. NERC recently was queried about this concern, and the response (which follows) was not especially reassuring: "Responsible Entities may choose to implement multi-impact rated programs to address low, medium, and high impact BES Cyber Systems. It is possible the same facts and circumstances

may indicate noncompliance of both the requirements applicable to low impact BES Cyber Systems and the corresponding requirements applicable to high and medium impact BES Cyber Systems. That the same act or omission may result in two separate violations is not unique to the CIP V5 standards. For example, the same failure to act immediately could constitute a violation of both TOP-001-1a R2 and TOP-008-1 R1. NERC's Sanction Guidelines provide that one penalty may be assessed where there are multiple violations arising from a single act or common incidence of noncompliance. Therefore, if a penalty is assessed at all, it would not be duplicated. In addition, the disposition of any noncompliance is based on the level of risk posed to the reliability of the BPS. Therefore, in the event one or more of the instances of noncompliance poses a minimal risk, a number of streamlined options is available, including treatment as a compliance exception. As with any noncompliance, a determination of whether compliance exception treatment will be appropriate in a given case will depend on the facts and circumstances." In particular, the reply by NERC staff cites examples in other Standards where a single omission or failure could violate two or more requirements of different Standards. It is Seattle's understanding, however, that addressing this 'double-standard' redundancy issue throughout the Standards is one of the objectives of the present Standards clean-up effort (as recommended by the Independent Experts report, P81 effort, the ongoing 5-year reviews, and the object of "world class" standards). In particular, the two TOP standards identified by NERC as examples today are being replaced with new TOP versions (in final ballot as this is written) that address this very 'double-standard' issue NERC cites as a 'reason' it's OK to have possible double jeopardy written into CIP v5. It is not OK. It is not world class. Newly written Standards should not include a known deficiency that industry resources now are being used to eliminate in other Standards. That NERC Saction Guidelines address potential aggregation of duplicative violations into a single penalty is welcome, but it treats the symptom of the problem rather than the cause.
Individual
Eric Ruskamp
Lincoln Electric System
No
The term Bulk Power System in the Rationale for Requirement R2 should be replaced with Bulk Electric System. The requirements outlined in Attachment 1, Element #4 for Low Impact assets are virtually identical to the requirements outlined in CIP-008-5 for High and Medium Impact BES Cyber Systems. While these requirements are appropriate for the High and Medium Impact BES Cyber Systems, they are overly onerous for the Low impact assets as the

requirements are not appropriately scaled to reflect the lower criticality of the assets the requirements are aiming to protect. This is especially true for the Low Impact assets that do not include External Routable Connectivity. These incident response requirements should only be required of High and Medium Impact BES Cyber Systems and therefore removed from Attachment 1, Element #4, or at minimum they should only apply to the Low Impact assets that have External Routable Connectivity. Without External Routable Connectivity, the only compromise to the BES is to the single BES Low Impact asset itself. According to the Rationale for Requirement R2, “these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised”. The Attachment 1 as written does not recognize the lower risk of the Low Impact BES assets.
Group
FirstEnergy
Mark Koziel
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does support EEIs recommendations for improving the wording of the requirements and related standards language.
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does support EEIs recommendations for improving the wording of the definitions and related standards language.
No
FirstEnergy does not agree that the CIP Standards adequately specify the scope of devices that can be classified as Transient Cyber Assets. The definitions and standard language make it unclear whether a Transient Cyber Asset needs to be treated as a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity makes a temporary routable connection between a Transient Cyber Asset and an ESP, would this Transient Cyber Asset also have to meet the requirements for the BES Cyber System or for a connected PCA? In other words, could the BES Cyber System requirements also be construed to apply to a Transient Cyber Asset that is temporarily connected? Recommendation: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) for 30 consecutive calendar

days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Transient Cyber Asset is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA)."
No
FirstEnergy does not agree that the CIP Standards adequately specify the scope of devices that can be classified as Transient Cyber Assets. The definitions and standard language make it unclear whether a Transient Cyber Asset needs to be treated as a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity makes a temporary routable connection between a Transient Cyber Asset and an ESP, would this Transient Cyber Asset also have to meet the requirements for the BES Cyber System or for a connected PCA? In other words, could the BES Cyber System requirements also be construed to apply to a Transient Cyber Asset that is temporarily connected? Recommendation: Change the definition for Transient Cyber Asset to: "A Cyber Asset that is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Transient Cyber Asset is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA)."
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does support EEIs recommendations for improving the implementation plan.
Yes
No Comment
No
No Comment
Group
MRO NERC Standards Review Forum
Joe DePoorter
Yes
CIP-003-6 R2 Att. 1 Element 2 – Recommend removing "based on need" for two reasons: 1. CIP-006-5 R1.1 – Requires controls to 'restrict' physical access, but it does not require authorizations or "based on need" for medium impact BES Cyber Systems that do not have External Routable Connectivity. This is an example of a requirement that is more prescriptive for low than for mediums because of the additional documentation associated with "based on need". 2. It is unclear how to interpret this part of the requirement due to the placement of the phrase "based on need", particularly with ", if any,". CIP-003-6 R2 Att. 1 Element 4 – Draft 2 added two more parts with 4.6 (record retention) and 4.7 (incident response plan updates.)

Recommend adding “if needed [required]” to 4.7. If the plan is okay, entities should not be required to update it.
Yes
Definitions – Low Impact BES Cyber System Electronic Access Point (LEAP) – Recommend replacing “allows” with “controls” Low Impact External Routable Connectivity (LERC.).
Yes
CIP-010-2 R4 Att. 1 Elements 1.2 and 3.1 – Recommend removing ‘Authorized’ because it adds requiring someone to approve/authorize these items. This additional level of documentation is more burdensome for low impact BES Cyber Systems. Entities would still be required to “specify” users, locations and use (individually or by group) for Element 1.2 and “specify” users and locations (individually or by group) for Element 3.1.
Yes
Yes
Yes
Yes
Implementation plan – Recommend changing the implementation date for physical access controls from April 1, 2018, to Sept. 1, 2018, because physical access controls must be applied to LEAPS, which don’t have to be identified until the electronic access controls implementation date of Sept. 1, 2018. CIP-010-2 Guidelines and Technical Basis Element 1.1 - Insert “type” with references to devices. For example, “…pre-authorize and inventory of devices or device types; or authorize devices or device types at the time….” CIP-011-2(X) R1.2 – Recommend going back to language similar to what was required in CIP-003 versions 3 and 4 R4.3, which stated: “The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.” There was no change from version 3 to version 4. The original version 5 mapping document indicates “no significant changes” when it was moved from CIP-003 to CIP-011 R1.3. However, R1.3 was removed from version 5 when the IAC language was incorporated. Now that IAC has been removed, the V3 text or something close to it should be retained. Possible revision: “The Responsible Entity shall, at least annually, assess adherence to its BES Cyber System Information protection program, including identification, protection and handling; document the assessment results; and implement an action plan to remediate deficiencies identified during the assessment.”
Individual
Karin Schweitzer
Texas Reliability Entity
No

1) Rationale for Requirement R1: Texas Reliability Entity, Inc. (Texas RE) recommends replacing “its” with “a Responsible Entity’s” in the second sentence of the first paragraph. The proposed revised language would read as follows: “The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity’s BES Cyber Systems.” 2) Requirement R1.2: Texas RE recommends the following elements be added to the Cyber Security Plan for Low Impact systems to reduce the risk to Medium and High Impact BES Cyber Systems: information protection, recovery functions, system security functions and configuration change management functions. By definition, Low Impact systems are those deemed not as critical to the BES as Medium or High Impact systems. However, in today’s integrated EMS networks, a vulnerability in a Low Impact system is imposed on Medium and High Impact BES Cyber Systems. Therefore the aforementioned items should be included in the Low Impact system Cyber Security Plans.
No
Low Impact BES Cyber System Electronic Access Point (LEAP): Texas RE requests the SDT consider including the functional definition that is already included in CIP-003-6, Attachment 1, Paragraph 3.1 within the proposed definition of a LEAP. In addition, we suggest striking the last sentence of the definition because it appears to be in conflict with the Electronic Access Control or Monitoring Systems (EACMS) definition that becomes effective April 1, 2016. The FERC approved EACMS definition includes all BES Cyber Systems and is not restricted to Medium or High Impact BES Cyber Systems; therefore, the LEAP definition should not exclude Low Impact BES Systems. Texas RE suggests the following change to the definition: “Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that allows Low Impact External Routable Connectivity and permits only necessary inbound and outbound access and denies all other access.”
No
1) Requirement R4: It appears the SDT may have inadvertently excluded low impact BES Cyber Systems. FERC directed in Order 791, Paragraph 136, that requirements should consider “processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact).” Texas RE recommends the following revision to Requirement R4: “Each Responsible Entity, for its high impact, medium impact, and low impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1, except under CIP Exceptional Circumstances.” 2) Measure 4: Proving compliance may be difficult for a registered entity since there is no requirement to maintain any identification nor connection records that validate whether the device was connected for 30 consecutive days. This could be remedied with the addition of the following language to M4: “including but not limited to a list of in-scope transient devices, and manual or automated logs showing connection periods…” The proposed revised language would read as follows: Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable elements in Attachment 1 and additional evidence, including but not limited to a list of in-scope transient devices, and manual or automated logs showing connection periods to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional

examples of evidence per element are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.
Yes
No
Texas RE suggests that the proposed implementation time periods are excessive by 12 months, particularly for administrative documentation. Therefore, Texas RE recommends the following changes for implementation for CIP-003-6: CIP-003-6: April 1, 2016 (no change) CIP-003-6, R1, R1.2: April 1, 2016 CIP-003-6, R2: April 1, 2016 CIP-003-6, Attachment 1, Element 1: April 1, 2016 CIP-003-6, Attachment 1, Element 2: April 1, 2017 CIP-003-6, Attachment 1, Element 3: September 1, 2017 CIP-003-6, Attachment 1, Element 4: April 1, 2016
Yes
No
Individual
David Jendras
Ameren
Agree
Ameren supports EEI comments for Project 2014-02 CIP V5 revisions.
Individual
Andrew Pusztai
American Transmission Company LLC
Yes
ATC has no comment.
Yes
ATC has no comment.
Yes
ATC has no comment.
Yes
ATC has no comment.
Yes
ATC appreciates the SDTs consideration of previous comments, and supports the adjustments in the implementation plan that accommodate for the time necessary to be successful in implementing elements 2 & 3 for Low Impact pursuant to CIP-003-6. Thank you.
Yes

ATC has no comment.
No
Individual
Oliver Burke
Entergy Services, Inc.
No
Entergy recommends aligning the Electronic Access Controls language with the Physical Access Controls language to allow the Responsible Entity the latitude to design controls that are consistent with needs dictated by the Responsible Entity's configuration.
No
In general, Entergy disagrees disagree with the creation of new acronyms that are applicable only to for Low Impact BES Cyber Systems.
Yes
Yes
Yes
Yes
No
Individual
Venona Greaff
Occidental Chemical Corporation
Yes
Occidental supports the structure of CIP-003-6, including Attachment 1.
Yes
Occidental supports the proposed new definitions of Low Impact External Routable Connectivity and Low Impact BES Cyber System Electronic Access Point. We appreciate the level of clarity that the two new definitions provide.
Abstain
Abstain
Yes

Occidental supports the tiered deadlines for the aspects of CIP-003-6 and believe them to be reasonable and appropriate.
Yes
Occidental supports the removal of the IAC language in the time frame ordered by FERC as well as the continued work by NERC to develop the Reliability Assurance Initiative.
No
Individual
Scott Berry
Indiana Municipal Power Agency
Yes
IMPA supports the SMUD comment on Attachment 1: SMUD does suggest an important edit to Attachment 1, Element 1 to clarify the obligation. The posted language requires “Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:…” Literal reading of this obligation means that entities are required to perform security awareness on a specific 15 month cycle. To align this obligation with that of CIP-004-5, R1, Part 1.1, SMUD requests the following edit: “Each Responsible Entity shall reinforce, AT LEAST ONCE every 15 calendar months, its cyber security practices, using one or a combination of the following methods.” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle.
No
IMPA supports the EEI comments regarding Attachment 2 of CIP-010-2: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped.
Yes
IMPA supports the removal of the wording and understands that NERC proposes to use the RAI program to keep these 17 requirements from becoming “zero” defect requirements. However, IMPA would like to see the RAI program be approved by the NERC Board and FERC before considering an “affirmative” vote on the CIP standards. In addition, the RSAWs need work with providing clarity and guidance for the compliance expectations of the CIP standards, especially since the IAC wording has been removed.
Individual

Candace Morakinyo
Wisconsin Electric Power Company
Agree
Edison Electric Institute (EEI)
Individual
Michelle D'Antuono
Ingleside Cogeneration LP
Agree
Occidental Chemical Corporation
Group
ACES Standards Collaborators
Trey Cross
Yes
The changes made to the formatting also assist entities in implementing the requirements through the use of attachment 1 and 2.
Yes
Yes
Additional guidance as to what is 'not' considered a transient device could be beneficial to the industry and would remove any possible confusion or assumptions.
Yes
Yes
We would like the drafting team to consider modifying the implementation dates for electronic access and physical security to be 18 months from the effective date of April 1, 2017. Physical security implementations, depending on the site(s), could have long durations and require additional budget cycles to implement across a diverse geographic and multiple asset types.
Yes
Moving from a zero defect compliance approach to a risk-based compliance is critical to the success of implementing CIP version 5. There has been significant progress made with Reliability Assurance Initiative. If RAI is not fully implemented and well understood by industry well in advance of the effective date of the CIP standards, there will be a significant increase in violations without a commensurate benefit to reliability. We are cautiously optimistic that RAI will be implemented in time for implementation of version 5 of the CIP standards.
Yes
(1) We support the CIP v5 Revisions Standards Drafting Teams' (SDT) efforts in minimizing the impact of Low Impact Facilities implementation by not requiring an asset inventory list,

allowing of grouping of assets for physical security and flexibility of restricting electronic access. (2) Because CIP Version 5 revisions will impact the smaller utilities, cooperatives, load serving entities, and distribution providers significantly, it is beneficial to these entities to approve CIP 5 revisions without further changes (so that they are steady-state) to allow for the impacted entities to plan, budget and implement CIP Version 5. (3) Approval of the changes to Identify, Assess, and Correct language removal, network communications security, Low Impact requirements and Transient Device requirements is recommended by ACES.
Individual
Amy Casuscelli
Xcel Energy
No
Xcel Energy has concerns about the requirements applicable to Low Impact assets. The revised language states that there is no expectation to keep a list of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users. It is unclear how compliance evidence of required electronic access controls per Attachment 1, Element 3 can be shown without such lists. Additionally, this appears to be in contradiction of the FERC directive to fix by adding specific requirements. It would seem the precedent used for Medium Impact without External Routable Connectivity of just documenting operational and procedural controls would be sufficient. This ambiguity in Requirement language is concerning since Xcel Energy will have over 600 low impact substations; an 850% increase in those subject to NERC CIP Compliance with a resulting significant financial impact to implement electronic access controls at these low impact substations. While the proposed standard allows an option or a combination of either access controls, monitoring or defining operational and procedural controls for Low Impact assets, these requirements are still beyond those of Medium Impact Assets without External Routable Connectivity. With these recommendations, it appears that more value is being placed on Low Impact Assets than Medium Impact without External Routable Connectivity so the Medium Impact Medium Impact without External Routable Connectivity language should be modified and/or Low Impact should follow the same requirements as Medium Impact without External Routable Connectivity. However, since Low Impact Assets are by definition those with low risk to the BES, the original Version 5 requirement simply requiring documentation of physical controls would seem sufficient. Given the number of Low Impact Assets, with the requirements in CIP-003-6 Attachment 1, more time will be spent addressing Low Impact facilities and assets than High or Medium. The R2 revision introduces a requirement to have ‘plans’ for each of the four areas for Low Impact systems. Previously the requirement was only to have policies/procedures/controls. This creates an additional administrative burden to bundle the policies/procedures/controls into a ‘plan’ and should be removed. Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. We recommend the addition of [if needed] after “180 calendar days.” Attachment 2 (examples of evidence) and Guidelines and Technical Bases for element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for element

2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistences make the language of the Standard in Attachment 1 vague and unclear. We recommend revising the Guidelines and Technical basis to include all example controls in one reference, and indicate that the minimum requirement for perimeter control shall include fences with locked gates and site access policies only. The language should indicate that additional controls, such as CCTV, card key access and special locks may be used as desired but exceeded the minimum requirement. In the Guidelines and Technical basis section the SDT uses the Version 3 term, special locks but outside of what is in the standard, does not define this term. Is a propriety key considered a special lock or what is the definition of “restricted keyway”?
No
The definitions for both LEAP and LERC are not clear. The LEAP definition would suggest that a logical network extends beyond a physical boundary, as the LEAP does not necessarily have to reside at the same location as the low-impact BES Cyber Systems. If the LEAP is not an EACMS, then what control is being applied to this asset classification? The definition for LERC is also unclear. The phrase “Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s).” is unclear if it is referring to access to/from a system or network.
Yes
Yes
No
We do not support the revised language providing for tiered deadlines for low impact assets.
Yes
One of the greatest advantages of the IAC language was to allow the industry to focus on security and move away from administrative burden of no to minimal risk issues. The idea of Internal Controls and RAI seems to be a good alternative, but has yet to be fully defined, leaving more burden on the industry, the regions and NERC to document and enforce minimal issues under the FFT program.
No
Individual
Megan Wagner
Westar Energy
Agree
Westar Energy supports the comments submitted by Edison Electric Institute (EEI).
Individual
Patrick Farrell

Southern California Edison Company
Yes
Yes
No
The revised language in CIP-010-2, Requirement 4 is unclear with respect to "under CIP Exceptional Circumstances." We would recommend revising the language to state: "Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1." We believe that this clarifies the language of this requirement. Additionally, SCE would suggest that Elements 1 and 2 of Attachment 1 be revised to clarify the levels of review required based on the control exercised by a Responsible Entity over a Transient Cyber Asset (TCA). The language should be revised to describe the requirements when an entity has "full" or "substantial" control through its ownership and management of the asset, as compared when an entity has "minimal" control, as seen when leasing an asset from a vendor. We think that this clarification would aid entities in ensuring compliance with CIP-010-2.
Yes
Yes
Yes
Yes
SCE strongly supports the EEI comments relating to CIP-010-2.
Individual
Chris Scanlon
Exelon Companies
No
Exelon supports the revised structure of CIP-003 and the extensive revisions made to the requirement language. Below are comments for SDT consideration. Exelon voted negative on CIP-003, though it feels the standard is very close to acceptable. While most of the comments point to refinements in the language rather than “deal breaker” concerns, the length of the list suggested that the standard is not yet ready for final approval. Exelon called out the most concerning issues below and feels that addressing all the points below will provide greater clarity for entities when the standard is implemented and audited. General Concerns 1.

Potential for Multiple violations: Exelon supports the use of CIP-003 for the requirements applicable to lows and appreciates the revised language that allows entities with multiple impact levels the option to incorporate low into related programs applicable to highs and mediums. This flexibility is important to accommodate the diverse circumstances that exist across the industry. However, Exelon has some concern that in a multi-impact rated program (high, medium and low), any failure to fulfill a requirement such as Attachment 1, Element 1 Cyber Security Awareness or Element 4 Cyber Security Incident Response, could result in violation of CIP-003-6, R2, CIP-004-5, R1 and CIP-008-5. Potential compliance and enforcement implications should not dictate the structure of the standards nor an entity's compliance program. An entity should be allowed to determine, in a form most efficient and effective to the entity, the best approach in fulfilling the security requirements. Please offer reassurance that the currently proposed structure with CIP-003-6, R2 does not create a potential situation for multiple violations. Confirmation from NERC Compliance will be important. This is a key concern that influenced a negative vote. 2.CIP-003-6, R2. Please directly discuss in the Guidelines the relevance of the "Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required." This note was important in the approval of V5 and Exelon supports inclusion of this note to help limit focus on a list of devices rather than emphasizing protections. However, many struggle to understand how to demonstrate compliance without having a list. Please discuss any potential alternatives to a list. As well, since the note does not preclude using a list if an entity determines this to be a desired tool to demonstrate compliance, please confirm that violations are not to accrue to the list, but only to failures to implement the plan Attachment 1 1.Element 1: To be consistent with CIP-004-5 and to match the discussion in the Guidelines, Element 1 should remove the word "its" to read: "Cyber security awareness: Each Responsible Entity shall reinforce, once every 15 calendar months, cyber security practices, using one or a combination of the following methods: …" 1a -The inclusion of "its" reads that the awareness program is to discuss the cyber security practices of the entity rather than the more general wording of CIP-004-5, R 1.1: "… reinforces cyber security practices (which may include associated physical security practices) …" Furthermore, addition of the parenthetical would be helpful to clarify that physical security practices are acceptable awareness topics under this requirement. These two adjustments are important to entities with multiple impact level BES Cyber Systems that may want to apply a single program to apply to high, medium and low impact levels. 1b - As well, the adjustment is needed to be consistent with the Guideline language: "The intent of the security awareness program is for entities to reinforce good cyber security practices … The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems." As stated, the intent does not limit the awareness topics to only those associated with internal cyber security policies and practices. 1c - This revision is important to Exelon and was a factor in the decision to vote negative. 2. Element 1: Please move the bullets under Attachment 1, Element 1 to Attachment 2, Element 2. Moving the bullets in the measures is consistent with CIP-004-5, R1.1. 3.Exelon supports the stand alone nature of the element 2 and 3 language. While the requirements in these elements are consistent with those in the corresponding requirements applicable to High and Medium impact BES Cyber Systems, it is

appropriate for those applicable to lows to be unique and appropriate to the risk presented by Low impact BES Cyber Systems. 4.Element 3: On electronic access controls, please offer more insight on “other electronic access controls that provide an equal or greater level of protection.” Exelon recognizes and appreciates that technology evolves and the requirement language should allow entities to use technology/methods that may prove useful in the future but not yet envisioned at the writing of the requirements. How does the drafting team envision that entities manage the comparison? 5.Element 4. Cyber Security Incident response: Please clarify the intent of “either by asset or group of assets…” Exelon pointed out in comments to the initial proposal that revision was needed to clarify that Cyber Security Incident response plans need not be site specific and that an enterprise-wide plan could fulfill the obligations for locations with low impact BES Cyber Systems. If this is the intent of the grouping language, Exelon supports the intent, but finds that the revision is not clear to that intent. If the intent is different, please explain and revise with clearer language. Consider the following revision: Cyber Security Incident response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s) covering either an individual asset or group of assets, which shall include: … Or just remove the comma after “plan(s)”. 6. Please justify the addition of 4.6 and 4.7 to the obligations of a Cyber Security Incident response plan. These elements were not required in the initial posting of the revisions and add an additional administrative burden to lows than was first proposed. Attachment 2 1.Exelon supports the use of Attachment 2 to provide added detail to the Measures. 2.See above for suggested move of Element 1 bullets from Attachment 1 to Attachment 2. 3.Element 1 – The wording can be clearer. Please consider the following revision (including the bullets from Attachment 1): “Element 1: An example of evidence for element 1 may include, but is not limited to documentation that cyber security practices have been reinforced once every 15 months through dated copies of the information used to emphasize security awareness via one or a combination of the following methods: Direct communications (for example, e-mails, memos, computer-based training); Indirect communications (for example, posters, intranet, or brochures); or Management support and reinforcement (for example, presentations or meetings).” Guidelines 1.Minor items: 1a - Page 33, Requirement R2 Attachment 1 – Physical Security, third paragraph, last sentence: Instead of “imply” consider require or obligate. 1b - Page 33, LEAP, third sentence, “LEAP” should be plural.
Yes
Yes
Exelon supports the proposed revisions to CIP-010-2. In our internal discussions, participants raised a couple questions. Exelon requests that the SDT consider incorporating responses to these questions either in a Q&A document or within the Guidelines. Below are the questions and draft responses from SDT outreach. Q and A Q1: Are contract obligations sufficient to fulfill the Element 2 requirements? A1: Yes, see Guidelines, in particular page 42: To facilitate these controls, Responsible Entities may choose to execute agreements with vendors and contractors to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department Of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. Elements

from the procurement language may unify vendor and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP Program elements may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the vendor's support. Entities should consider the elements of the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls. Q2: How often are entities required to scan Removable Media to fulfill element 3.2? A2: Frequency and timing of scanning was intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The Removable Media must be scanned before it is connected to the BES Cyber Asset and that timing as dictated by the entity's plan should reduce the risk of malicious code mitigation.
Yes
Yes
Exelon supports the currently proposed Implementation Plan. We understand that others in the industry prefer to sync up the deadlines for the physical and electronic access control requirements. While Exelon would accept synced deadlines, it would do so only if the physical access controls deadline moved out to September 1, 2018 to match the electronic access controls deadline. Exelon prefers the staggered approach over moving the electronic access control deadline up to April 1, 2018. In addition, Exelon requests that the SDT consider incorporating responses to a question on the implementation plan either in a Q&A document or within the Guidelines. Below is a question and draft response from SDT outreach. Q and A Q1: Under the Cyber Security Incident response plan required to be in place by April 1, 2017, would a physical access incident be an incident if the physical access controls are not required until April 1, 2018? Likewise for electronic access controls not required until September 1, 2018? A1: The April 1, 2017 deadline requires that entities have a response plan in place. Since lows are not required to have ESPs or PSPs, the operative trigger is whether an event occurred that "Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System" (per the second bullet). As written in the implementation plan, between April 1, 2017 and the respective implementation deadlines for access controls, the entity would be required to demonstrate response to incidents that meet the second bullet; however, would not have to demonstrate the implementation of access controls that may have been related to the incident.
Yes
Exelon supports the Version X package of revisions and understands the need to have these revisions approved should they need to go forward independent of the revisions for Low Impact and Transient Devices. However, Exelon strongly supports the SDT's efforts to complete revisions in all four issues areas by the Feb 2015 filing deadline and hopes for a break in the revisions to the CIP standards. CIP resources are currently devoted to implementation of CIP Version 5. The task is daunting and resource intensive. Exelon looks forward to a stretch of time in which CIP work can focus on implementation without revisions

in development. In addition, timely resolution of the Order 791 CIP-003 directive is important to enable entities to avoid an iterative implementation of V5 and V6 for the Low Impact assets.
Yes
Concerns remain with the implications of the CIP-003 requirements on dispersed generation. Exelon supports the progress of the Order 791 revisions, but would like to see continued collaboration with the Project 2014-01 Applicability for Dispersed Generation Resources Standards to better balance the demonstration of compliance burden with the risk of dispersed generation facilities. Exelon thanks the SDT for their hard work in revising the CIP standards.
Individual
David Rivera
New York Power Authority
No
NYPA recommends that the language added to CIP-003-6, table R2 (Low Impact Assets) be moved to the specific tables in each of the Standards CIP-004-6 through CIP-011-2 where applicable. The inclusion of these control requirements for Low Impact Assets, as an Attachment to CIP-003-6, results in Standards language inconsistencies that creates confusion and is likely to cause additional compliance risks to entities having multiple impact levels. The following are some specific examples: A. The Low Cyber System requirements continue to be inconsistent with High / Medium requirements in other standards. These current inconsistencies have been attributed to deficiencies in the Quality Assurance process used prior to the release of this new draft, however, this only validates concerns that there will 'always' be inconsistencies of this type when the controls are split between the Standards as was done in this case. B. The shifting of the Low impact requirements to CIP-003-6, R2, breaks one of the prime objectives defined when CIP version 5 was being developed that each of the Standards (except CIP-002) be able to stand on its own. At entities with Low and either Medium or High Cyber Systems, it would be necessary that CIP-003 always be referenced when any of the requirements in CIP-004-6 through CIP-011-2 are being designed and implemented, since dependencies are always possible between Cyber Systems that are part of any impact category. This could also lead to the following: 1. If a BES asset contains Low and Medium or High Cyber Systems, it would be possible to violate multiple requirements in multiple Standards. This would be clearly be possible for some of the requirements in CIP-004, CIP-006 and CIP-008 (or any Standard with a facility impact), since having some 'Low's along with any other impact level Cyber Assets would apply to all Cyber Assets in that facility. 2. This further complicates the new policy and procedure structures that an entity needs to meet CIP version 5 compliance. The NIST-like structure outlined in CIP-003, R1, is likely the most common direction that most entities will choose to 'clearly' meet CIP Version compliance. Having the 'Low' impact Cyber Systems hanging 'out on a limb' in a CIP-003 Attachment will reduce the clarity of addressing the required controls for those assets in a 'mixed'-impact environment. The end of result of having Low Impact Asset controls contained only in CIP-003

is that going forward, as the CIP requirements are changed, the likelihood of creating additional inconsistencies is high. For example, if a slight change is made to a requirement in CIP-007-6, which somehow affects the set of Low Cyber Systems, then having to make a similar change to CIP-003-6, R2, in accounting for that change, may result in the change being missed and/or becoming inconsistent. These new set of CIP standards are already very complex, and any added confusion caused by this structural problem will result in difficult (and costly) compliance implementations. This will likely negate the goals of improving overall reliability.
No
We agree with the NPCC cpmments on this question.
No
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Group
PJM Interconnection LLC
Stephanie Monzon
Yes
Yes
Yes
Yes
Yes
Yes
No

Individual
Sonya Green-Sumpter
South Carolina Electric & Gas
Individual
Kalem Long
The Empire District Electric Company
Agree
EEI
Individual
Christina Conway
Oncor Electric Delivery Company LLC
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions. Additional comments below: CIP-010-2 R4 Attachment 1: Oncor utilizes embedded device platforms, such as Substation relays and RTUs, which are not as vulnerable to malicious code/Malware as computer systems. It is Oncor's interpretation that Substation embedded device platforms are afforded security features provided by nature of embedded controls. However, these embedded devices do not have access control or logging capabilities, therefore incapable to log users and/or generate logs. Therefore, it is not technically feasible to demonstrate that a specific Transient Device, such as a laptop, is connecting or was connected to such embedded device platform. CIP-010-2 R4 Attachment 1 Element 1.2.2: The Guidelines and Technical Basis page 44 Element 1.2.2 states: To meet this requirement part, the entity is to document the following: 1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations. As previously mentioned, it is not technically feasible to authorize locations for Transient Devices, such as laptops, to access substation cyber assets. There are controls in place to restrict access such

as perimeter fence with locked gates, locked control house doors, and unique passwords to the assets. Oncor is seeking clarity on the following: Does the section on page 43 “Per Cyber Asset Capability” exclude the aforementioned Medium Impact BES Cyber Assets without ERC substation assets based on capabilities? Recommendation: Rewrite the Requirement, Attachment(s) and/or Guideline and Technical Basis to clarify and articulate that embedded device platforms, such as substation relays and RTUs, which are not vulnerable and incapable of control accessing or logging, are excluded from CIP-010-2. Alternatively, Limit applicability to Medium Impact BES Cyber Assets with ERC, or vulnerable to malicious code.
Yes
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
Yes
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
Yes
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
Group
Duke Energy
Michael Lowman
Yes
No
Duke Energy suggest the following revision to Low Impact BES Cyber System Electronic Access Point: “Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that permits Low Impact External Routable Connectivity. The Cyber Asset may reside at a location external to the asset or assets containing low impact BES Cyber Systems. The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System except when the LEAP is on the same Cyber Asset as an Electronic Access Control or Monitoring System.” We believe the use of the word “allows” is too broad whereas the word “permits” better reflects the SDT’s intent. The addition of “except when the LEAP is on the same Cyber Asset as an Electronic Access Control or Monitoring System” is needed for those instances when a LEAP is on the same Cyber Asset as an Electronic Access Control or Monitoring System.
No
Duke Energy suggests adding a time requirement in Attachment 2, section 1 similar to the one found in Attachment 1 section 1. As currently written, there does not appear to be a time requirement for the frequency with which an entity should review Transient Cyber Assets owned or managed by Vendors or Contractors. Is an entity required to review the items listed in section 2.1 every time a vendor logs on/ patches into the Cyber Asset?

Yes
We ask the SDT to provide an example of a device the is not capable of transmitting executable code. We are unclear as to an example of a Transient Cyber Asset that is not capable of transmitting executable code.
No
Duke Energy suggests revising the Compliance Date for CIP-003-6, Attachment 1, element 2 to coincide with the Compliance Date of CIP-003-6, Attachment 1, element 3. As currently written, it appears that the elements are circular in nature. Essentially, an entity would need to be compliant with element 3 before becoming compliant with element 2 and could be physically protecting a device that does not exist.
Yes
No
Group
Southern Company: Southern Company Services, Inc.; Alabama Power Company, Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Pamela Hunter
No
Southern appreciates the substantial revisions to the requirements language in CIP-003 and Attachment 1 and offers several items for SDT consideration below. The new structure and overall content are a great improvement. The negative vote on CIP-003 is only to address these couple of issues but overall the newly drafted standard reflects the appropriate level of detail for requirements applicable to Low Impacts assets. Comment 1: CIP-003-6 – Attachment 1: CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation: Change Attachment 1, Element 2 to “Physical security controls” to be consistent with the language of the standard. Please edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs) to CIP-003-6 R1 for consistency. Comment 2: CIP-003-6 Requirement R2 ends with “include the elements in Attachment 1”, although the first sentence in Element 1 says “include each of the elements provided below” the actual “elements” are not labelled “elements” as in Attachment 2, which references the elements in Attachment 1. Recommendation: Add “Element” before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses. This would also be helpful for Attachment 1 in CIP-010-2. Comment 3: The “(LERC)” and “(LEAP)” acronyms are missing in Element 2, 3, and 3.1, which makes it harder to identify the use defined phrases in these elements. Recommendation: Add the “(LERC)” and “(LEAP)” to elements 2, 3, and 3.1 to make it easier to identify the acronym. Comment 4: CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation: Add “,

if needed," after "180 calendar days." Comment 5: CIP-003-6 Attachment 2 and Guidelines and Technical Basis for element 2: Attachment 2 (examples of evidence) for element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for element 2 states "entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control." These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation: Include "perimeter controls" under element 2, Attachment 2 in the example: "(e.g., card key, special locks, perimeter controls). Comment 6: CIP-003-6 Guidelines and Technical Basis for Requirement R2 Attachment 1 and the LERC definition – Electronic Access Controls: The following scenario is unclear: {Low impact BES Cyber System (e.g., control system) ---- |1| ---- Cyber Asset (e.g., data historian) ---- |2|} ---- Location X Where: {} represents the asset/site boundary, |1| represents a firewall or electronic access point (in this case firewall 1), and ---- represents a bi-directional routable communication Based on the language of the definition and CIP-003-6 it is unclear whether there is a LERC and LEAP in this scenario and if there is LERC, which firewall is the LEAP. The Guidelines and Technical Basis for CIP-003-6 say "the electronic access controls should address the risk of using the asset's LERC to gain access to the low impact BES Cyber Systems." However, this scenario would require an adversary to gain access to not one but two access points, the firewalls on either side of the Cyber Asset (firewall 2 and then firewall 1) to get access to the low impact BES Cyber System. Whereas, the examples provided all show one access point, the LEAP, which requires controls. Recommendation: Add this scenario to the CIP-003-6 Guidelines and Technical Basis, clarify that there is a LERC and allow the Responsible Entity to have the flexibility choose the LEAP, either firewall 1 or firewall 2. Comment 7: The Guidance on LEAP has the phrase "However the LERC between assets "behind" the LEAP and another asset containing a low impact BES Cyber System must also pass through the single LEAP". LERC between assets behind the LEAP" could imply connectivity between them is allowed without passing through the LEAP first – regardless of their communications with another asset containing a low impact BES Cyber System (which by definition would have to be behind a LEAP as well, but maybe not the same one). Southern Recommendation: Consider rephrasing to: However the LERC between assets "behind" the LEAP must pass through the single LEAP. Comment 8: The Guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation: In the Guidelines and Technical Basis for CIP-003-6, where LEAP is described, move the sentence "LEAP are not to be considered EACMS…" to create a second paragraph and add "However a LEAP can be implemented within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself."

No

Southern appreciates the new terms to help clarify the requirements language in CIP-003. The negative vote on CIP-003 is only to address these couple of issues. Comment 1: Use of “allows” in the LEAP definition does not allow for the use of an unmanaged hub. An unmanaged hub, which does not support access controls and may be acting as a central connecting point, could be considered an interface that “allows” Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs. Recommendation: Change “allows” to “controls” to allow for the use of unmanaged hubs as appropriate. Please also make sure this is changed in the Guidelines and Technical Basis and anywhere else the LEAP definition is provided. Comment 2: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation: Change the exclusion sentence to: “Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).” Alternatively, clarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to include point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions.
No
Southern appreciates the revisions and overall direction that SDT made to the structure of CIP-010-2, R4 but offers the comments for consideration below to help with clarity. Comment 1: CIP-010-2 Attachment 1: The use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and 2) it is implied by the language of 1.2 and 1.3. The language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization. The redundancy creates uncertainty in the interpretation of the standard. It could be interpreted to imply a second step in addition to the R4 plan. In other words, in addition to the R4 plan for Transient Cyber Assets and Removable Media, which includes the 1.2 and 3.1 authorization elements, the Responsible Entity must also have a separate, formal approval process to identify authorized users, authorized locations, and authorized uses for Transient Cyber Assets and a separate formal approval process to identify who is authorized to use and where they are authorized to use Removable Media. We believe the intent of the Standards Drafting Team is that the plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address these authorization elements. This flexibility will allow the Responsible Entity to either write a plan that specifically defines who is authorized to use the Transient Cyber Asset(s) for which uses and locations or include a separate authorization process, which may include a formal approval process, in the plan that identifies the users, locations, and uses authorized for the Transient Cyber Asset(s). It will also give the Responsible Entity the same flexibility for Removable Media authorizations. This flexibility is particularly needed for

Responsible Entities that rely on contractor use of Responsible Entity managed Transient Cyber Assets and Removable Media who have less control over the contractor, i.e., the control is defined by a service agreement or contract. Giving the Responsible Entity flexibility on how to define the authorization process will allow them to align these requirements with their vendor contracts. Recommendation: Remove “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. Alternatively, clarify in the Guidelines and Technical Basis under Element 1.2 and 3.1 that the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 does not require a formal approval process for each user, location, and use of the Transient Cyber Asset (or Removable Media), but gives the Responsible Entity the flexibility to develop an authorization plan that either directly defines authorization or requires a specific authorization process. This allows Responsible Entities to align their Transient Cyber Asset and Removable Media authorizations with their vendor contracts for use of Responsible Entity managed Transient Cyber Assets. Comment 2: CIP-010-2- Attachment 1 Elements 1 and 2 are grouped by whether a Transient Cyber Asset is owned or managed by the Responsible Entity or by a vendor or contractor. The intent of this grouping is good because it considers the level of control by the Responsible Entity. However, the actual groupings could result in a Transient Cyber Asset that falls under both element 1 and 2. For example, if a Responsible Entity owns the Transient Cyber Asset, but a contractor manages its use under a service management contract. Another scenario is that the vendor owns the Transient Cyber Asset, but the Responsible Entity manages it. For these scenarios, it is unclear whether the Responsible Entity should include element 1 or 2 or both elements in their R4 plan(s). Recommendation: Remove “Owned or” from elements 1 and 2. Comment 3: CIP-010-2 Attachment 1, section 1.5: Currently drafted as: Transient Cyber Asset resides within a location with restricted physical access; Recommendation: Consider rephrasing to say: The Transient Cyber Asset must reside within a location with restricted physical access; Comment 4: CIP-010-2 - Attachment 1, Element 2.3: “Responsible Entities shall determine whether additional mitigation actions are necessary…” requires a statement that says no additional mitigation measures were identified as necessary, which creates an unnecessary administrative burden. Also, Element 2.3 is an element that should be addressed by the R4 plan for Transient Cyber Assets and Removable Media, the way Element 2.3 is written makes it look like a requirement rather than a plan element, which also causes confusion as to the frequency of review for elements 2.1 and 2.2. Element 2.3 as written suggests that a Responsible Entity must use the 2.3 and 2.4 mitigation methods prior to each connection of a vendor-owned Transient Cyber Asset in order to determine whether additional mitigation measures will be needed. This can be overly burdensome and unnecessary when a vendor is moving from system to system in a single day. Also, a Transient Cyber Asset may be owned by the Responsible Entity and managed by a vendor or owned by the vendor/contractor and managed by the Responsible Entity. The use of “vendor- or contractor-owned” in 2.3 is not consistent with these scenarios (see comment 3.3 above). Recommendation: Add “necessary” before “such actions.” Also, clarify in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how to manage vulnerability and malicious code reviews of their vendors or contractors and require additional mitigation actions. For example, one entity may require a vendor to plug a Transient Cyber Asset into a kiosk to scan for vulnerabilities and malicious code before each

connection. However, this approach may not be feasible for all entities, so defining a process to initially and periodically check and audit vendor/contractor processes for vulnerability and malicious code mitigation. Specifically, “prior to connecting the vendor- or contactor-owned Transient Cyber Asset” does not require that 2.1, 2.2, and 2.3 before each connection, but that the Responsible Entity should define a process to manage the use of vendor- or contractor- managed Transient Cyber Assets to mitigate vulnerabilities and malicious code. Also, change “owned” in 2.3 to “managed.” Comment 5: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped. Recommendation: Make it clear in the Guidelines and Technical Basis that “mitigate” and “mitigation” does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system that the Transient Cyber Asset or Removable Media is used on. Also, it may be impossible to detect every piece of malicious code. Mitigation is meant to reduce security risks, but elimination of all risk is impossible. Comment 6: CIP-010-2 – Attachment 2, Element 3.2: This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. Recommendation: Change “scan Removable Media outside of the BES Cyber System” to “use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code.” Comment7: Guidelines and Technical Basis for R4, Attachment 1, Element 1.1: inventories of Transient Cyber Assets is allowed by individual or group – individually or by asset type, therefore language under Element 1.1 should be consistent, allowing inventory of devices or device type. Recommendation: Add “or device types” to the second sentence: “pre-authorize and inventory of devices or device types or authorize devices or device types at the time of connection or use a combination of these methods.”

No

Comment 1: Transient Cyber Asset Definition: The “and” in the parenthesis after “A Cyber Asset,” is confusing and appears to be misplaced. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. It refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, “directly connected” may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Recommendation: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3)

a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.” Also, if the intent is for the Transient Cyber Asset definition to apply to both routable and non-routable communications, clarify this in the Guidelines and Technical Basis for CIP-010-2.
No
Southern appreciates the revised schedule and supports the increased timeframe for implementation. The only reason for the negative vote is the disconnect between the dates as noted below. Comment 1: CIP-003-6, Attachment 1, Element 2 compliance date of April 1, 2018: According to the Implementation Plan, the Element 2 physical access controls must be applied to LEAPs by April 1, 2018; however, the LEAPs are identified under Element 3, which must be applied by September 1, 2018. Recommendation: The compliance date for LEAPs is after the compliance date for physical, but the two are tied together since LEAPs have to be physically secured. These two dates should be the same or please add clarity on how best to implement the requirements based on disconnect between the two timeframes.
Yes
Southern supports the Version X package of revisions.
Yes
Southern would like to commend the SDT for all the hard work and effort that has gone into revising the CIP Standards.
Individual
Muhammed Ali
Hydro One
Agree
Task Force on Infrastructure Security & Technology - TFIST
Individual
Bob Thomas
Illinois Municipal Electric Agency
Agree
Florida Municipal Power Agency
Individual
John Merrell
Tacoma Power
Agree
Sacramento Municipal Utility District
Individual
David Burkey
Puget Sound Energy
Agree
Edison Electric Institute

Individual
David Thorne
Pepco Holdings Inc
Yes
PHI supports EEI Comments for this question.
Yes
Further clarification and description of the time sensitivety associated with LERC should be included in the Guidelins and Technical Basis section.
Yes
PHI supports EEI Comments for this question.
Yes
PHI supports EEI Comments for this question.
Yes
Yes
Yes
PHI supports EEI Comments for this question.
Individual
Roger Dufresne
Hydro-Quebec Production
No
Incoherence with CIP-002-5 are observed. Elements of CIP003-6 R2 are base on new definitions that applies to elements explicitely excluded from CIP-002-5. CIP-005 need to be ajusted to reflect the real intentions of the SDT. Incoherence are observed for the implementation dates: CIP-003-6, Attachement 1,element 1 until the later of April 1, 2017 CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 Physical requirement (element 2) goes in effect before the electronic ones (element 3). Requirement 2 demands to restric acces point of low BCS while low BCS a covered 5 months later.
Yes
No
Impacts are major for the utilities
Yes

No
See answer to question 1
Yes
No
Individual
Brett Holland
Kansas City Power and Light
No
No, we do not agree. The protections suggested for low impact assets still represent too large a pool of assets that do not have a substantive impact to the BES, the reference to electronic and physical controls language required for low impact assets is vague and open to much interpretation, and the requirement for issues to be reported to the ES-ISAC does not support measured improvement for reliability and security of the BES.
No
The new definitions do not add clarity, but rather confusion and complexity. Entities will be better served by describing the connectivity to their assets and how the entity manages security and reliability of those assets. Entities should explain how they mitigate risk and manage assets in support of BES reliability.
No
KCP&L, in agreement with SPP, offers the following comments. Item 1.2 in Attachment 1 contains requirements already covered in other standards. An authorized user will be on the entity's list required by CIP-004-6 Requirement 4. Thus, Item 1.2 is not needed. Also, this standard does not define when actions should take place. Clarification is needed and should be placed for industry vote on requirements addressing a Vendor's Transient Cyber Assets.
Yes
No
KCP&L, in agreement with SPP comments, offers the following comments. While additional time to complete tasks resulting from changes in the standard is welcome, the number of dates to manage is not. There should be one date for High and Medium Impact BES Cyber Assets and their accompanying devices and one for Low Impact BES Cyber Assets and associated devices. We would recommend that the latest date for each grouping be chosen as a new effective date for all requirements.
Yes
No

Group
Florida Municipal Power Agency
Carol Chinn
Yes
SMUD does suggest an important edit to Attachment 1, Element 1 to clarify the obligation. The posted language requires “Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:…” Literal reading of this obligation means that entities are required to perform security awareness on a specific 15 month cycle. To align this obligation with that of CIP-004-5, R1, Part 1.1, SMUD requests the following edit: “Each Responsible Entity shall reinforce, AT LEAST ONCE every 15 calendar months, its cyber security practices, using one or a combination of the following methods.” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle.
Yes
FMPA supports EEI’s comment regarding the definition of a LEAP: The definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation: In the Guidelines and Technical Basis for CIP-003-6, on page 42 of 49 where LEAP is described, move the sentence “LEAP are not to be considered EACMS…” to create a second paragraph and add “However a LEAP can be implemented within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself.”
No
FMPA supports EEI’s comment regarding Attachment 2 of CIP-010-2: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped.
Yes
FMPA supports SMUDs comments regarding Transient Cyber Assets and Removable Media: SMUD agree with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. However, SMUD is concerned with starting the definition of Removable Media with the capitalized “Media” considering that “Media” is itself not a defined term. SMUD recommends an edit to resolve this concern: Removable Media: One or more media directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, or access data. Removable

Media are not Cyber Assets. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Yes
FMPA supports SMUDs comments for CIP-006-6: SMUD agrees and supports the proposed implementation plan deadlines for CIP-003-6, R2. SMUD appreciates that the SDT has provided a tiered approach to the implementation of physical security and electronic access controls. SMUD believes that even with the tiered approach to the implementation plan, entities are not restricted from implementing both controls in parallel. Considering the diverse nature of the facilities and systems, SMUD believes the additional compliance time as well as the tiered approach provides entities the needed flexibility to evaluate their physical security and system capabilities to effectively apply the new requirements. There are possibilities that physical modifications will need to be made to facilities to deploy the necessary controls to restrict physical access. Additionally, to deploy a Low Impact Electronic Access Point, it is possible that certain systems or computer network architectures may need to be modified to accommodate the additional of an access point.
No
The SDT has done an excellent job of addressing the IAC language along with their outreach and addressing stakeholder comments. FMPA can agree with the removal of the IAC language, but unfortunately, the current RSAWs do not provide enough clarity and guidance on compliance expectations to understand if “zero tolerance” concerns have been addressed. There is substantive work that needs to be done on the RSAWs, especially in light of the removal of the IAC language and the fact that RAI program documents have just been recently released and RAI is in early implementation stages. It’s not clear that RAI will address the “zero tolerance” concerns since there is processing and reporting required for 100% of non-compliance. More clarity around the RAI program may address this but it’s not clear at this point. The RSAWs are also a tool to address this matter.
Yes
FMPA’s negative votes are due to the current condition of the RSAWs and the status of RAI implementation. We expect that affirmative votes can be cast if : a. Compliance staff collaborates with the SDT on the RSAW revisions for the next posting that will significantly improve the RSAWs and b. if more clarity is communicated around how RAI addresses “zero tolerance”. FMPA also supports EEI’s comments regarding CIP-007-5: CIP-007-6 R2: Can you violate 2.3 while you meet 2.4? If you identify a patch within 35 days of evaluation and create a dated mitigation plan that says 8 months, but then 2 months later, the implementation of the patch is delayed a month because you can’t take the system down, the plan under 2.3 is no longer valid and you cannot revise it under 2.3 since 35 days have passed; however, under 2.4 you can revise the plan so 2.4 is not violated. Is 2.3 violated in this case?
Individual
Cliff Johnson
Consumers Energy Company

No
We agree with all except the two items below: Not as written specific to CIP-003-6 Attachment 1 numbers 3 and 4.7. Number 3 has the potential to create significant undue burden on entities. This language begins to treat Low Impact assets as if they could have some sort of significant impact on the BES and begins to approach the compliance activities that are applicable to more significant Medium and High Impact assets. Many entities own a significant number of geographically dispersed Low Impact assets with a multitude of cyber asset types making compliance with this language very time and resource intensive. If this level of compliance activities is mandated, the associated implementation deadline would need to be significantly delayed. This also increases the risk of losing focus on the Medium and High Impact assets. Number 4.7 requires updating the plan within 180 days after a test or actual incident without mention of a need for a change being identified that would drive the update. What update is an entity expected to make if the plan is well designed and the test or response to an actual incident was completely successful? We suggest modifying 4.7 to require the update of the plan when corrections or improvements are identified during a test or response to an actual incident.
Yes
Yes
Yes
No
Not as written specific to CIP-003-6 Attachment 1 number 3, it needs to be adjusted according to entity feedback.
Yes
No
Individual
Rich Salgo
NV Energy
No
The SDT made significant improvements to the language and the structure of these Requirements. There remain a few inconsistencies and clarification items that are potential trouble spots which necessitate a negative ballot. These are listed below: Attachment 1: The language in Element 1 “using one or a combination of the following” is inconsistent with the Element 2 language “through one or more of the following.” We recommend the SDT change the language in Element 1 to “through one or more of the following.” CIP-003-6 Requirement

R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” We recommend the SDT change Attachment 1, Element 2 to “Physical security controls” to be consistent with the language of the standard. This would extend to all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs). Attachment 1, Element 4.7 assumes the response plan will always need updates, which may not be the case. We recommend to add the important clarifier “if needed,” after the words “180 calendar days.” Beyond the changes outlined above, we note that the nature of the changes for CIP-003-6 to accommodate the Commission’s directive on Low Impact cyber assets hinge on the new terms introduced in this posting (LERC and LEAP). As noted in the following question response, we are advising several important changes to these terms. Without some assurance that these changes will be adopted, we cannot determine the suitability of CIP-003-6 and therefore cannot cast an affirmative ballot amid the uncertainty of the resolution on these definitions.
No
LEAP: The use of the word “allows” in the LEAP definition is not compatible with the use of an unmanaged hub. Such an unmanaged hub, which does not support any access controls and may be merely acting as a central connecting point, would be considered an interface that “allows” Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs and would therefore be problematic for compliance with this requirement. We recommend the SDT change the word “allows” to “controls”, which will therefore exclude unmanaged hubs from any requirements involving LEAPs. LERC: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. We recommend to change the exclusion sentence to: “Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).”
No
In Attachment 1, the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and (2) it is already implied by the language of 1.2 and 1.3. The language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which amounts to an “authorization.” The redundancy creates uncertainty in the interpretation of the standard, and could call into question whether a second step of authorization is prescribed. We recommend the removal of the word “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 as well as appropriate clarification in the Guidelines and Technical Basis. In Attachment 2, Element 3.2 is too restrictive and does not serve to mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. We recommend that the SDT change “scan

Removable Media outside of the BES Cyber System" to "use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code."
Yes
Yes
We generally support the implementation plan as a whole; however, there appears to be a conflict between the date for which LEAPs are to be identified under Element 3 and the date that physical access controls are to be applied to these LEAPs (Sept 1, 2018 for the former; April 1, 2018 for the latter).
Yes
Individual
Kara Douglas
NRG Energy
Yes
Yes
Yes
Yes
Yes
Yes
suggest the SDT remove all "shalls" in the Attachment and refer to it as a list of items to include in a program.
Yes
For Version-X proposed changes: suggest the SDT remove all "shalls" in the Attachment and refer to it as a list of items to include in a program.
Group
SPP and specific Members
Lesley Bingham
Yes

No
The new definitions do not add clarity, but rather confusion and complexity. There is audit risk for an entity if their interpretation of these terms differs from that of their Compliance Enforcement Authority. Most entities will be better served by describing the connectivity to their assets through a policy statement which can be crafted to address a specific location.
No
Item 1.2 in Attachment 1 contains requirements already covered in other standards. An authorized user will be on the entity's list required by CIP-004-6 Requirement 4. Thus, Item 1.2 is not needed. Also, this standard does not define when actions should take place. Should a Vendor's Transient Cyber Asset and processes be reviewed every time the Vendor touches and entity's systems? Annually? Once and then not again? Clarification is needed on this point.
Yes
No
While additional time to complete tasks resulting from changes in the standard is welcome, the number of dates to manage is not. There should be one date for High and Medium Impact BES Cyber Assets and their accompanying devices and one for Low Impact BES Cyber Assets and theirs. We would recommend that the latest date for each grouping be chosen as a new effective date for all requirements.
No
The removal of the IAC language has been closely tied to the proposed Reliability Assurance Initiative (RAI). While that program can, ideally, allow for auditors to review an entity's controls which will identify, assess, and correct issues, the RAI program is not complete and has not been used in the audit and enforcement process. Simply put, this requires a significant amount of trust. The IAC language provides a more clear path and boundaries for auditors.
No
Individual
Brenda Hampton
Luminant Energy Company, LLC
Agree
Luminant Generation Company, LLC
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No

MMWEC respectfully submits the following suggestions for clarifying and improving the CIP-003-6 Attachments 1 and 2. Attachment 1, Element 1: change "once every 15 calendar months" to "at least once every 15 calendar months." In Attachment 2, Element 1 - change "once every 15 calendar months" to "at least once every 15 calendar months" or delete "once every 15 months. Attachment 1, Element 2: It is not clear whether the phrase "based on need" refers to the need to restrict physical access or the need to allow certain physical access. Does it mean that entities are required to restrict access by default and justify any allowed access? The Attachment 2 example for Element 2 indicates that an entity must describe the operational need for physical access, but also contains the confusing phrase "restrictions cited above are based on need" implying that it is the "restriction" that must be justified and documented. Please clarify. Attachment 1, Element 4.1: Change "Identification, classification, and response to Cyber Security Incidents" to "Identification and classification of Cyber Security Incidents." Delete “response” because "response" is a sub-set of "incident handling" which is required by Element 4.4. Attachment 1, Element 4.3: Since testing of the Cyber Security Incident Response Plan is required only every 36 months, entities should be required to ensure that individuals are aware of their response roles through more frequent training or review of their responsibilities. Consider modifying Element 4.3 to require those groups and individuals to review their roles and responsibilities for Cyber Security Incident response at least once every 15 months. Attachment 2, Element 3: Change "(e.g. IP addresses, ports, services)" to "(e.g., by restricting IP addresses, ports and/or services)" and move this phrase to follow "deems necessary" later in the same sentence. It is not clear from the current wording whether an entity must restrict using all of the example attributes.

No

MMWEC is concerned with the use of the phrase “low impact BES Cyber System.” Shouldn’t this be “BES Cyber Systems associated with Low Impact assets?” For the definition of LERC, consider changing “Communication protocols created…” to “Communication using protocols created…”

No

MMWEC respectfully submits the following suggestions for improving the CIP-010-2 Attachment 1. CIP-010-2, Attachment 1 should be limited to requiring control objectives not specific controls. Bullets are example controls and should not be include in Attachment 1 requirements. These examples should be moved to Attachment 2 or to guidance. CIP-010, Attachment 1, Element 1.1 is a method of compliance rather than a control objective. It is unnecessary and should be deleted from Attachment 1 and moved to guidance. The following is recommended wording for control objectives for Attachment 1 Elements 1.3, 1.4, 1.5, 2.1 and 2.2: "1.3 - Each Responsible Entity shall mitigate security vulnerabilities on Transient Cyber Assets." “1.4 Each Responsible Entity shall mitigate the risk of introduction of malicious code (per Transient Cyber Asset capability.)” “1.5 Each Responsible Entity shall mitigate the risk of unauthorized use of Transient Cyber Assets.” “2.1 Each Responsible Entity shall mitigate the risk of security vulnerabilities (per Transient Cyber Asset capability.)” “2.2 Each Responsible Entity shall mitigate the risk of introduction of malicious code (per Transient Cyber Asset capability.)” Using control objectives for elements 2.1 and 2.2, element 2.3 is redundant and should be deleted from Attachment 1. CIP-010, Attachment 1, Element 3.2 –

Change entire element to "Each Responsible Entity shall mitigate the risk of introduction of malicious code associated with the use of Removable Media." The examples of how to do this (i.e., scanning) could be included in Attachment 2 or guidance.
No
It not clear whether a Cyber Asset that meets the definition of BES Cyber Asset could be categorized as a Transient Cyber Asset (and require only the controls for Transient Cyber Assets) if it is connected for less than 30 days. To clarify that it cannot be classified as a Transient Cyber Asset, MMWEC recommends adding the following sentence to the end of the definition of Transient Cyber Asset,: "A Cyber Asset that meets the definition of BES Cyber Asset shall not be categorized as a Transient Cyber Asset." Another approach to this issue would be to restrict application of the Transient Cyber Asset category by changing the last sentence to “Transient Cyber Assets are limited to Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.”
Yes
Yes
No
Group
Edison Electric Institute (EEI)
Melanie Seader
No
EEI appreciates the efforts of the Standard Drafting Team (SDT) in revising CIP-003-6 to meet stakeholder concerns. We believe CIP-003-6 is close, but not yet ready for final ballot due to the following comments. We encourage the SDT to consider all of these comments carefully as our members have worked hard to explain their concerns in these comments as well as provide specific recommendations to help the SDT. Comment 1.1: CIP-003-6 Rationale for Requirement R2: “Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised.” Aggregating low impact BES Cyber Systems across multiple assets does not reflect a true risk-based assessment and therefore this sentence is not accurate. Recommendation 1.1: Delete this sentence. Comment 1.2: CIP-003-6 – Attachment 1: The language in Element 1 “using one or a combination of the following” is inconsistent with the Element 2 language “through one or more of the following.” Recommendation 1.2: Change the language in Element 1 to “through one or more of the following.” Comment 1.3: CIP-003-6 – Attachment 1: CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation 1.3: Change Attachment 1, Element 2 to “Physical security controls” to be

consistent with the language of the standard. Please edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs) to make them consistent with the CIP-003-6 R1 language. Comment 1.4: CIP-003-6 Requirement R2 ends with "include the elements in Attachment 1," although the first sentence in Element 1 says "include each of the elements provided below" the actual "elements" are not labelled "elements" as in Attachment 2, which references the elements in Attachment 1. Recommendation 1.4: Add "Element" before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses. This would also be helpful for Attachment 1 in CIP-010-2. Comment 1.5: The "(LERC)" and "(LEAP)" acronyms are missing in Element 2, 3, and 3.1, which makes it harder to identify the use of these defined terms in these elements. Recommendation 1.5: Add the "(LERC)" and "(LEAP)" to elements 2, 3, and 3.1 to make it easier to identify the terms. Comment 1.6: CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation 1.6: Add ", if needed," after "180 calendar days." Comment 1.7: CIP-003-6 Attachment 2 and Guidelines and Technical Basis for Element 2: Attachment 2 (examples of evidence) for Element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for Element 2 states "entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control." These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation 1.7: Include "perimeter controls" under Element 2, Attachment 2 in the example: "(e.g., card key, special locks, perimeter controls). Comment 1.8: CIP-003-6 Guidelines and Technical Basis, Requirement R2 Attachment 1 bold text subtitles on page 32: The subtitles are inconsistent with the element language in Attachment 1. Recommendation 1.8: Change the subtitle language to "Requirement R2 Attachment 1 – Cyber Security Awareness" and "Requirement R2 Attachment 1 – Physical Security Controls" (see Comment and Recommendation 1.3 above).

No

Comment 2.1: Use of "allows" in the LEAP definition does not allow for the use of an unmanaged hub. An unmanaged hub, which does not support access controls and may be merely acting as a central connecting point, could be considered an interface that "allows" Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs. Recommendation 2.1: Change "allows" to "controls" to allow for the use of unmanaged hubs as appropriate. Please also make sure this is changed in the Guidelines and Technical Basis and anywhere else the LEAP definition is provided. Comment 2.2: Because the acronyms LEAP and LERC are used to help simplify the terms defined and used in the standard, it would help to include the acronyms each time the terms are spelled out in full in the definitions and in the standards and related guidance. Recommendation 2.2: Insert the acronyms "(LERC)" and "(LEAP)" as they are spelled out in the definitions. Comment 2.3: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation 2.3: Change the exclusion sentence to: "Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication

protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols)." Also, clarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to include point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions. Comment 2.4: The definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation 2.4: In the Guidelines and Technical Basis for CIP-003-6, where LEAP is described, move the sentence "LEAP are not to be considered EACMS…" to create a second paragraph and add "However a LEAP can be implemented within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself." Comment 2.5: Based on the LERC definition and the CIP-003-6 Guidelines and Technical Basis for Requirement R2 Attachment 1 – Electronic Access Controls, the following scenario is unclear: {Low impact BES Cyber System (e.g., control system) ---- |1| ---- Cyber Asset (e.g., data historian) ---- |2|} ---- Location X Where: {} represents the asset/site boundary, |1| represents a firewall or electronic access point (in this case firewall 1), and ---- represents a bi-directional routable communication Based on the language of the definition and CIP-003-6 it is unclear whether there is a LERC and LEAP in this scenario and if there is LERC, which firewall is the LEAP. The Guidelines and Technical Basis for CIP-003-6 say "the electronic access controls should address the risk of using the asset's LERC to gain access to the low impact BES Cyber Systems." However, this scenario would require an adversary to gain access to not one but two access points, the firewalls on either side of the Cyber Asset (firewall 2 and then firewall 1) to get access to the low impact BES Cyber System. Whereas, the examples provided all show one access point, the LEAP, which requires controls. Recommendation 2.5: Add this scenario to the CIP-003-6 Guidelines and Technical Basis, clarify that there is a LERC and allow the Responsible Entity to have the flexibility choose the LEAP, either firewall 1 or firewall 2.

No

EEI appreciates the efforts of the Standard Drafting Team (SDT) in revising CIP-010-2 to meet stakeholder concerns. We believe CIP-010-2 is close, but not yet ready for final ballot due to the following comments. We encourage the SDT to consider all of these comments carefully as our members have worked hard to explain their concerns in these comments as well as provide specific recommendations to help the SDT. Comment 3.1: CIP-010-2 R4: The placement of "under CIP Exceptional Circumstances," is awkward. Recommendation 3.1: Move "under CIP Exceptional Circumstances" up in the sentence, such that it reads "…shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s)…" Comment 3.2: CIP-010-2 Attachment 1: The use of "Authorized" in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and 2) it is implied by the language of 1.2 and 1.3. The language of 1.2

and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization. The redundancy creates uncertainty in the interpretation of the standard. It could be interpreted to imply a second step in addition to the R4 plan. In other words, in addition to the R4 plan for Transient Cyber Assets and Removable Media, which includes the 1.2 and 3.1 authorization elements, the Responsible Entity must also have a separate, formal approval process to identify authorized users, authorized locations, and authorized uses for Transient Cyber Assets and a separate formal approval process to identify who is authorized to use and where they are authorized to use Removable Media. We believe the intent of the Standards Drafting Team is that the plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address these authorization elements. This flexibility will allow the Responsible Entity to either write a plan that specifically defines who is authorized to use the Transient Cyber Asset(s) for which uses and locations or include a separate authorization process, which may include a formal approval process, in the plan that identifies the users, locations, and uses authorized for the Transient Cyber Asset(s). It will also give the Responsible Entity the same flexibility for Removable Media authorizations. This flexibility is particularly needed for Responsible Entities that rely on contractor use of Responsible Entity managed Transient Cyber Assets and Removable Media who have less control over the contractor, i.e., the control is defined by a service agreement or contract. Giving the Responsible Entity flexibility on how to define the authorization process will allow them to align these requirements with their vendor contracts. Recommendation 3.2: Remove “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. Also, clarify in the Guidelines and Technical Basis under Element 1.2 and 3.1 that the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 does not require a formal approval process for each user, location, and use of the Transient Cyber Asset (or Removable Media), but gives the Responsible Entity the flexibility to develop an authorization plan that either directly defines authorization or requires a specific authorization process. This allows Responsible Entities to align their Transient Cyber Asset and Removable Media authorizations with their vendor contracts for use of Responsible Entity managed Transient Cyber Assets. Comment 3.3: CIP-010-2-Attachment 1 Elements 1 and 2 are grouped by whether a Transient Cyber Asset is owned or managed by the Responsible Entity or by a vendor or contractor. The intent of this grouping is good because it considers the level of control by the Responsible Entity. However, the actual groupings could result in a Transient Cyber Asset that falls under both element 1 and 2. For example, if a Responsible Entity owns the Transient Cyber Asset, but a contractor manages its use under a service management contract. Another scenario is that the vendor owns the Transient Cyber Asset, but the Responsible Entity manages it. For these scenarios, it is unclear whether the Responsible Entity should include element 1 or 2 or both elements in their R4 plan(s). Recommendation 3.3: Remove “Owned or” from elements 1 and 2. Comment 3.4: CIP-010-2 - Attachment 1, Element 2.3: “Responsible Entities shall determine whether additional mitigation actions are necessary…” requires a statement that says no additional mitigation measures were identified as necessary, which creates an unnecessary

administrative burden. Also, Element 2.3 is an element that should be addressed by the R4 plan for Transient Cyber Assets and Removable Media, the way Element 2.3 is written makes it look like a requirement rather than a plan element, which also causes confusion as to the frequency of review for elements 2.1 and 2.2. Element 2.3 as written suggests that a Responsible Entity must use the 2.1 and 2.2 mitigation methods prior to each connection of a vendor-owned Transient Cyber Asset in order to determine whether additional mitigation measures will be needed. This can be overly burdensome and unnecessary when a vendor is moving from system to system in a single day. Recommendation 3.4: Add "necessary" before "such actions." Also, clarify in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how to manage vulnerability and malicious code reviews of their vendors or contractors and require additional mitigation actions. For example, one entity may require a vendor to plug a Transient Cyber Asset into a kiosk to scan for vulnerabilities and malicious code before each connection. However, this approach may not be feasible for all entities, so defining a process to initially and periodically check and audit vendor/contractor processes for vulnerability and malicious code mitigation. Specifically, "prior to connecting the vendor- or contactor-owned Transient Cyber Asset" does not require that 2.1, 2.2, and 2.3 before each connection, but that the Responsible Entity should define a process to manage the use of vendor- or contractor- managed Transient Cyber Assets to mitigate vulnerabilities and malicious code. Comment 3.5: CIP-010-2 – Attachment 1, Element 2.3 : A Transient Cyber Asset may be owned by the Responsible Entity and managed by a vendor or owned by the vendor/contractor and managed by the Responsible Entity. Therefore the use of "vendor- or contractor-owned" in 2.3 is not consistent with these scenarios (see Comment and Recommendation 3.3 above). Recommendation 3.5: Change "owned" in 2.3 to "managed." Comment 3.6: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of "mitigate" and "mitigation" should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped. Recommendation 3.6: Make it clear in the Guidelines and Technical Basis that "mitigate" and "mitigation" does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system that the Transient Cyber Asset or Removable Media is used on. Also, it may be impossible to detect every piece of malicious code. Mitigation is meant to reduce security risks, but elimination of all risk is impossible. Comment 3.7: CIP-010-2 – Attachment 2, Element 3.2: This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. Recommendation 3.7: Change "scan Removable Media outside of the BES Cyber System" to "use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code." Comment 3.8: CIP-010-2 – Attachment 2, Element 1.2: The second sentence under Element 1.2 is a restatement of Attachment 1, Element 1.2 and is not an example of evidence. Recommendation 3.8: Remove the second sentence under Attachment 2, Element 1.2: "The documentation must…" to keep the text in Attachment 2 focused on examples of evidence and not include requirements. Comment 3.9: Guidelines and Technical Basis for R4,

Attachment 1, Element 1.1: Inventories of Transient Cyber Assets is allowed by individual or group – individually or by asset type, therefore language under Element 1.1 should be consistent, allowing inventory of devices or device type. Recommendation 3.9: Add “or device types” to the second sentence: “pre-authorize and inventory of devices or device types or authorize devices or device types at the time of connection or use a combination of these methods.”
No
Comment 4.1: Transient Cyber Asset Definition: The “and” in the parenthesis after “A Cyber Asset,” is confusing. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. Also, the parenthetical for the examples is misplaced; it refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and, therefore, unclear as to which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, “directly connected” may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Recommendation 4.1: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.” Also, if the intent is for the Transient Cyber Asset definition to apply to both routable and non-routable communications, clarify this in the Guidelines and Technical Basis for CIP-010-2.
Yes
The timeframes in the implementation plan are reasonable and appropriate; however, we have the following comment to help clarify a source of confusion among Responsible Entities: Comment 5.1: CIP-003-6, Attachment 1, Element 2 compliance date of April 1, 2018: According to the Implementation Plan, the Element 2 physical access controls must be applied to LEAPs by April 1, 2018; however, the LEAPs are identified under Element 3, which must be applied by September 1, 2018. This requires Responsible Entities to identify LEAPs before April 1, 2018, which may be unclear under the Implementation Plan. Recommendation: Clarify in the Implementation Plan that the LEAPs must be identified before April 1, 2018 in order to apply physical access controls to them by April 1, 2018.
Yes
No
Individual

Thomas Foltz
American Electric Power
No
The modification of CIP-003-6 R1 exceeds FERC's order to add "objective security controls" to R2 in the existing approved standard. The inclusion of item 1.2 in requirement R1 to create a cybersecurity policy adds an additional burden on Entities that have facilities with low impact BES Cyber Systems. The previous draft only required the documentation and implementation of cyber security plans under R2 that addressed the defined items. The additional compliance burden of creating and maintaining another policy document under R1 will not provide an appreciable increase in cyber security to the BES. The documentation and implementation of cyber security plans that include “objective criteria” to evaluate the sufficiency of an entity’s protections as ordered by FERC should be sufficient. AEP suggests the SDT revert to the original wording of R1 and add the "objective criteria" to R2. In CIP-003-6, Attachment 1 Item #2, the language is more prescriptive than the wording for Medium Impact BES Cyber Systems without External Routable Connectivity. AEP suggests the wording be modified to provide a level of flexibility for low impact BES Cyber Systems that is commensurate with their potential impact to the BES. For example, regarding physical security, it may be difficult to prove compliance with this section given the options provided. This may necessitate installing card readers on over 1,000 substations. AEP suggests removing the prescriptive bullet points, “Access controls; Monitoring controls; or Other operational, procedural, or technical physical security controls,” and similar prescriptive language. Separating the security controls into Attachment 1 and what appears to be a combination of examples, measures, and evidence into Attachment 2 in CIP-003-6 is confusing and a deviation from the formatting of the other CIP standards. AEP suggests that the wording be transferred to a table similar to the rest of the CIP standards. Regarding the CIP-003-6 R2 rationale “Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised,” aggregating Low Impact BES Cyber Systems across multiple assets does not reflect a true risk-based assessment. Rather, the existing Standard focuses on individual Assets that contain Low Impact BES Cyber Systems. FERC did not order a change in this philosophy. AEP suggests deleting this sentence.
No
The definitions create confusion where they refer to "asset" when it appears the term should be "facility." AEP suggests changing the second lowercase use of the word "asset" in each definition to be "facility."
No
Separating the security controls into Attachment 1 and what appears to be a combination of examples, measures, and evidence into Attachment 2 in CIP-010-2 is confusing and a deviation from the formatting of the other CIP standards. AEP suggests that the wording be transferred to a table similar to the rest of the CIP standards. AEP is concerned with the use of the term “security vulnerabilities,” which AEP believes is a broader term than, e.g., security

patch management or malicious code prevention utilized in CIP-007. AEP disagrees with the implication that a Responsible Entity would be required to mitigate “security vulnerabilities,” which may require Responsible Entities to monitor the National Vulnerability Database and address all vulnerabilities published over a day, week, month, or year where there are currently 65,268 security vulnerabilities. Large corporate networks are not able to address all security vulnerabilities in real time. How can this be expected on Transient Cyber Assets that may or may not have External Routable Connectivity? AEP suggests reverting to, e.g., security patch management or malicious code prevention rather than “security vulnerability mitigation.” This would align with the CIP-007 requirements and would be a more reasonable and manageable requirement. The existence of External Routable Connectivity should also be taken into consideration when revising this requirement to ensure the CIP standards treat devices commensurate with their risk profile. Element 3.2 of Attachment 1 is too restrictive. This presumes the scanning takes place on another system. The capabilities exist today to have embedded virus scan and encryption on USB drives. This should not require the scanning of the USB drive on a system outside the BES Cyber System as the scanning is taking place in real time by the applications running on the USB drive itself. Consider how this requirement relates to CIP-007 R3, where a Responsible Entity is required to “deploy method(s) to deter, detect, or prevent malicious code.” The methods deployed on a BES Cyber System would cover the threat of malicious code introduced via Removable Media. There is more than one layer of security controls that protects a BES Cyber System from the threat of malicious code introduced via Removable Media. Physical security, user account management, BES Cyber System software patch management, and BES Cyber System malicious code prevention, for example, are all required and would provide significant threat mitigation against the introduction of malicious code via Removable Media. The technology to prove compliance with the scanning requirement prior to connecting Removable Media to a BES Cyber System is not readily available. Systems are not equipped to provide the granularity as to what USB drive, CD/DVD, memory card, or floppy disk has been plugged into it. AEP suggests revising the requirement to allow the use of more advanced Removable Media with the ability to scan for malicious code during use without the burden of additional scanning requirements on external systems. Regarding Element 1.2 of Attachment 1, authorization and verification of users on Transient Cyber Assets is not practical when the Transient Cyber Assets do not have External Routable Connectivity or are not connected to a BES Cyber System with External Routable Connectivity. The authorization and verification of users, locations, and uses of Transient Cyber Assets without External Routable Connectivity would be a paper exercise with no technical means of enforcement or logging. As a result, without External Routable Connectivity, it is not possible to verify that the risks of Transient Cyber Assets were properly mitigated. This authentication would be a significant administrative burden with negligible reliability benefit (similar to those Requirements removed during the Paragraph 81 effort) when considering the significant number of BES Cyber Systems and Assets that will be in scope. AEP suggests that the element be modified to only require the authorization of users and approved transient hardware for the ESP accessible via a network to high or medium impact BES Cyber Systems with External Routable Connectivity. Regarding Element 2 of Attachment 1, vendors and contractors are not subject to CIP requirements themselves. A

Responsible Entity cannot force a vendor or contractor to adhere to the requirements of this element. Use of specialized vendor expertise and tools may be limited such that BES reliability would be impacted. Imposing this requirement on vendors and contractors is in fact more restrictive than medium impact BES Cyber Systems with External Routable Connectivity. AEP suggests removing Element 2 in its entirety.
No
Regarding Transient Cyber Assets, the 30 day timeframe prevents a Responsible Entity from being able to consider a device that is temporarily connected to the BES Cyber System as part of the BES Cyber System, and it is arbitrarily beyond what was ordered by FERC. AEP suggests removing the 30 day timeframe to reduce the amount of tracking Responsible Entities must do with respect to these devices.
No
AEP is concerned that the tiered approach to effective dates is overly complicated and will create confusion, especially for large entities. AEP suggests streamlining the implementation date to the latest date proposed in the Version X and Version 6 implementation plans.
Yes
While AEP supports this approach, AEP is also expecting that NERC and the regions will continue to implement the Reliability Assurance Initiative to embody the spirit of the "IAC" language. For example, AEP expects to continue to see self-logging privileges granted for lower risk items pursuant to the criteria set forth by the RAI.
Yes
AEP recommends that the drafting team not include a prescriptive approach in the proposed attachments in CIP-003 and CIP-010. Such prescriptive approaches unreasonably restrict the Responsible Entities from defining their own programs. For those items where the drafting team has proposed prescriptive approaches, AEP recommends removing them from an "Attachment" format and including them in tabular format as requirements similar to the remainder of the CIP Requirements without the prescriptive elements of the steps Responsible Entities are required to take. While AEP understands that this approach creates a baseline for cybersecurity in the industry, it is also concerned about the security of prescribing one approach for all companies within a critical infrastructure sector which could increase the likelihood of a successful attack across a broad front. AEP recommends including the exclusion from the defined term “Low Impact External Routable Connectivity” for transfer trip communications into the defined term “External Routable Connectivity.” Exclusion wording from LERC definition: “Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).” There is no mandated timeframe to address the low impact and transient cyber device directives. AEP urges the SDT to take the time necessary to ensure that the requirements achieve the necessary reliability benefit and that there is broad-based industry support.
Individual
Barry Lawson

National Rural Electric Cooperative Association (NRECA)
In CIP-003-6, R2, it states “Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.” NRECA strongly supports this statement. In order to help registered entities to better understand how this “Note” can be used in demonstrating compliance, NRECA requests that the SDT explain and provide examples on how registered entities can comply with this standard without providing a list for audit purposes. NRECA requests that the SDT provide a detailed justification for the most recent additions of 4.6 and 4.7 to CIP-003-6, Attachment 1. These elements were not included in the first posting of the CIP V5 revisions and they have been added without adequate justification. These two new requirements add additional compliance and administrative burdens compared to the first posting without a demonstration of why they are needed for BES reliability. While NRECA will be voting in the affirmative, we expect the SDT will fully address why these requirements are needed for BES reliability. If this cannot be done, then 4.6 and 4.7 should be removed from Attachment 1.
Yes
Yes
Yes
While NRECA supports the proposed Implementation Plan, we request that the SDT consider syncing up deadlines for the physical and electronic access control requirements so that both are required by September 1, 2018.
Yes
NRECA supports the Version X package of revisions. However, we are very hopeful that the SDT can successfully complete revisions to CIP V5 that address FERC’s four directives by the Feb 2015 filing deadline. Having the four directives addressed by the filing deadline is critical to achieving a steady state for the CIP standards.
Yes
NRECA appreciates the efforts of the CIP V5 Revisions SDT in addressing this challenging project under very tight time constraints.
Individual
Nathan Mitchell
American Public Power Association
Agree
Scott Saunders - SMUD
Group
Iberdrola USA
John Allen

No
Support EEI comments And The revised structure of CIP-003-6 has made it more cumbersome, and confusing to use. The use of the table in the previous version was effective. Attachment 1 is a list of requirements and should be treated as such within the main body of the standard.
No
Support EEI comments
No
Support EEI comments AND As written, Attachment 2.3 requires each Entity to review each vendor's policies/procedures. Recommend changing from "Responsible Entities shall determine whether additional mitigation actions are necessary" to "Responsible Entities may determine whether additional mitigation actions are necessary"
Yes
Support EEI comments
Yes
Yes
No
Group
BC Hydro
Patricia Robertson
No
The cyber security plan elements defined within Attachment 1 are deemed to be too detailed and excessive for Low Impact BES Cyber Assets.
Yes
No
a) BC Hydro recommends a revision to the detailed expectations on the Responsible Entity in relation to Attachment 1, 2 Transient Cyber Asset(s) owned or managed by Vendors or Contractors. It is anticipated that it will not be feasible to actively review and monitor the measures on devices not owned by the Responsible Entity as detailed in Attachment 1, 2. b) BC Hydro recommends a revision to the expectations with regard to Attachment 1, 3 Removable Media. The revision would provide clarity on authorized users (ie is this applicable for vendors as well as the Responsible Entity).
No

BC Hydro requests clarification regarding the language "… directly connected for 30 calendar days or less …" Does this mean if a Responsible Entity has a USB drive plugged in to a BES Cyber Asset continuously for 32 days, that device no longer represents Removable Media?
N/A
Yes
Although BC Hydro overall supports the removal of the IAC language, it will create a zero-tolerance with regards to items of non-compliance. For high risk items this is appropriate however for low risk items the IAC language would be appropriate.
Yes
BC Hydro recommends a definition or guidance be developed with regards to the term "cyber security plan"
Individual
Andrew Ginter
Waterfall Security Solutions Ltd.
No
Almost all USB flash drives, mice, keyboards and other devices contain CPUs and software. Attackers can physically modified such devices to attack the computers to which the devices are connected - see http://www.theregister.co.uk/2011/06/27/mission_impossible_mouse_attack/ for an example. Worse, a malware-infected computer can compromise the software running in some kinds of connected USB devices - see http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/ for an example. Thus, a USB flash stick or other device whose firmware is compromised while connected to an external computer can cause BES Cyber Assets to malfunction when the USB drive is connected to those assets, either by loading malware on to the BES Cyber Asset, or by issuing incorrect mouse or keyboard commands to the asset. This suggests that USB devices generally should be considered BES Cyber Assets or Transient Cyber Assets, but the Removable Media definition gives USB flash drives as an example of Removable Media. The definitions and examples should make it clearer whether USB keyboards, mice, flash drives and other CPU & software-containing USB devices are BES Cyber Assets, Transient Cyber Assets, or Removable Media, and why those types of USB devices should be classified in this manner.
Group
PacifiCorp

Sandra Shaffer
No
o Need definition modifications completed before voting YES. PacifiCorp also supports the comments of MidAmerican Energy Company regarding dispersed generation resources.
No
o LERC definition: The second sentence uses undefined terms that cause confusion and refers to specific technologies which over time will make the definition obsolete as technologies change. This exception also seems to remove protections indiscriminately rather than addressing the importance of the assets to be protected and finding ways to provide meaningful controls around them without impacting the effectiveness of the protocols in question.
No
o Attachment 1, Element 1.2: Recommend removing ‘Authorized’ because it adds requiring someone to approve/authorize these items. Entities would still be required to “specify” users, locations and use (individually or by group) for each part in Element 1.2. It also should be noted that the physical location that the Transient Device is approved for may not be as relevant as the logical network or cyber system that the Transient Device is used with (i.e. there may be multiple networks available at a particular location and which network it’s used on is more impactful to the Transient Device than the physical location itself). Consider changing element 1.2.2 to specify “network zones or cyber systems, either individually or by group, that the Transient Device may be used with.” o Attachment 1, Element 3.1: Recommend removing ‘Authorized’ because it adds requiring someone to approve/authorize these items. Entities would still be required to “specify” users and locations (individually or by group) for each part in Element 3.1.
Yes
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
Yes
TSGT feels that the “topics” of R1 should reflect the “elements” of Attachment 1 referenced in R2 unless there is a different meaning intended with the different wording. If so, please clarify the difference. One way to do this would be to simply refer to Attachment 1 under R1.2 and remove all the sub-requirements under R1.2.
Yes

Yes
No
TSGT believes that the recent revisions made to the Removable Media and Transient Cyber Asset definitions introduced some unintended ambiguity. Revisions should be made to make it clear what the assets/devices must be connected to, in order to clarify this qualifier of the definition. It is our understanding that the intent of the drafting team was to state "…directly connected… [clause]… to…", where the items after the "to" is what the "Cyber Asset" or "Media" is connected to. One simple solution is to add a comma after the [clause] and before the word "to". Another option is to state the [clause] part after the list of what the "Cyber Asset" or "Media" is connected to. Here is a suggested revision to how the definition for Removable Media might read: A Cyber Asset, directly connected to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) ; and connected for 30 consecutive calendar days or less, capable of transmitting executable code. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Yes
The timelines are fine, but written in a very convoluted way. It would be helpful to state them more succinctly.
Yes
No
Group
Bonneville Power Administration
Andrea Jessup
BPA supports SMUD's comments with the exception of Questions 2 and 5.
Yes
BPA supports SMUD's comments.
Yes
BPA believes that reusing the term Access Point within the new definition of Low Impact BES Cyber System Electronic Access Point leads to confusion with existing medium and high definitions.
Yes
BPA supports SMUD's comments.
Yes
BPA supports SMUD's comments.
Yes

BPA disagrees with the tiered implementation timeline as currently proposed. BPA believes more time is required to create practices and procedures to implement the policy effectively. BPA suggests that policy (CIP-003-6, R1, part 1.2) be implemented prior to other requirements (CIP-003-6, R2 and CIP-003-6, R2 Attachment 1, items 1-4).
Yes
BPA supports SMUD's comments.
Yes
BPA disagrees with the CIP-007-6 R1.2 expansion of scope to non-programmable communication components and proposes re-alignment to R1.1. To increase the potential for managing compliance to this requirement, BPA requests additional guidance defining the specific nonprogrammable communication components located inside both a PSP and an ESP. This clarification is requested in addition to what has already been added via the Guidelines illustration and Technical Basis section.
Individual
Randi Nyholm
Minnesota Power
Agree
Minnesota Power supports comments submitted by EEI related to CIP-003-6, CIP-010-2 and the implementation plan.
Individual
Joe Tarantino
Sacramento Municipal Utility District
Yes
SMUD agrees and supports the changes that were made to CIP-003-6, R2 including the use of Attachment 1 and Attachment 2. SMUD does suggest the following changes: The posted language in Attachment 1, Element 1 requires “Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:…” Literal reading of this obligation means that entities are required to perform security awareness on a specific 15 month cycle. To align this obligation with that of CIP-004-5, R1, Part 1.1, SMUD requests the following edit: “Each Responsible Entity shall reinforce, at least once every 15 calendar months, its cyber security practices, using one or a combination of the following methods.” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle. The posted language in CIP-003-6, R1, Part 1.2, Subpart 1.2.2 uses “Physical Security Controls” to define the policy obligation. However, in Attachment 1, Element 2, “Physical access controls” is used. SMUD recommends Attachment 1, Element 2 be changed to “Physical security controls” to be consistent with the language in CIP-003-6, R1. Additionally, edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, and RSAWs). The posted language in Attachment 1, Elements 2, 4, and 3.1 do not use the acronyms for Low Impact BES Cyber System Electronic Access Point or for Low Impact External Routable Connectivity. SMUD

recommends that the acronyms “LEAP” and “LERC” be used after each of their defined terms. The posted language in Attachment 1, Element 4, Part 4.7 requires that the Cyber Security Incident Response Plan be updated “within 180 days” of a test or actual incident. SMUD recommends add “if necessary” after “within 180 days.” It is possible that no updates are actually needed to the plan following either event and it should not be necessary for entities to update a document unless there is a need to make improvements. The posted language in Attachment 2, Examples of Evidence for Element 2 provides card key and special locks as examples of physical security controls; however, the Guidelines and Technical Basis for Element 2 states, “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” SMUD recommends including “perimeter controls” under Attachment 2, Element 2 as an example “(e.g. card key, special locks, perimeter controls)” for consistency. The posted language in Attachment 1, Element 3, requires the use of a Low Impact BES Cyber System Electronic Access Point (LEAP) if there is Low Impact External Routable Connectivity (LERC). The definition of a LEAP is the “interface” of the device that “allows” the LERC. SMUD recommends that the Guidelines and Technical Basis for Attachment 1 where LEAP is described be updated to include statements that the LEAP can be implemented within the same Cyber Asset that is serving the function of an EACMS or EAP designated for a high impact or medium impact BES Cyber System. This is acceptable because regardless of the impact rating, it is the “interface” that is in scope. It is not the intent to require entity’s to have two separate physical Cyber Assets for either access point implementation. Potential for Multiple violations: SMUD has some concern that in a multi-impact rated program (high, medium and low), any failure to fulfill a requirement, such as Attachment 1, Element 1 Cyber Security Awareness or Element 4 Cyber Security Incident Response could result in violation of CIP-003-6, R2 as well as CIP-004-5, R1 and CIP-008-5. Potential compliance and enforcement implications should not dictate the structure of the standards nor an entity’s compliance program. An entity should be allowed to determine, in a form most efficient and effective to the entity, the best approach in fulfilling the security requirements. Please offer reassurance that the currently proposed structure with CIP-003-6, R2 does not create a potential situation for multiple violations. Confirmation from NERC Compliance will be important to reassure industry. Can NERC Compliance explain how this issue would be addressed under the Reliability Assurance Initiative?
Yes
SMUD supports the new definitions for Low Impact External Routable Connectivity and Low Impact BES Cyber Systems Electronic Access Point. SMUD appreciates the development of new definitions to simplify the language in the requirement. SMUD does suggest the following minor changes to the definitions for clarity: The posted language for the Low Impact BES Cyber System Electronic Access Point (LEAP) definition uses “allow” in regards to Low Impact External Routable Connectivity (LERC), SMUD recommends using the word “controls” to be specific that it is the intent of the interface of the LEAP to control the communication inbound and outbound for the asset(s) containing the low impact BES Cyber System.
Yes

SMUD agrees and supports the changes that were made to CIP-010-2, R4; including the use of Attachment 1 and Attachment 2. SMUD does recommend a few edits for clarity: The posted language for Attachment 1, Element 2.3 requires, “Responsible Entities shall determine whether additional mitigation measures are necessary…” which is intended to ensure that entity’s make an affirmative decision to allow the device to connect. SMUD recommends adding “if necessary” after “additional mitigation actions” for clarity to ensure that entities can accept the device without requiring modifications. The posted language for the Transient Cyber Assets in Attachment 1, Element 1 allows for authorization to be done individually or by asset type; however the Guidelines and Technical Basis for Element 1 does not discuss the ability to authorize based on a group of assets. SMUD recommends language be added to allow “authorization individually or by groups of assets” to the Guidelines and Technical Basis for Element 1.1.
Yes
SMUD agree with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. However, SMUD is concerned with starting the definition of Removable Media with the capitalized “Media” considering that “Media” is itself not a defined term. SMUD recommends an edit to resolve this concern: “Removable Media: One or more media”, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, or access data. Removable Media are not Cyber Assets. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Yes
Comments: SMUD agrees and supports the proposed implementation plan deadlines for CIP-003-6, R2. SMUD appreciates that the SDT has provided a tiered approach to the implementation of physical security and electronic access controls. SMUD believes that even with the tiered approach to the implementation plan, entities are not restricted from implementing both controls in parallel. Considering the diverse nature of the facilities and systems, SMUD believes the additional compliance time as well as the tiered approach provides entities the needed flexibility to evaluate their physical security and system capabilities to effectively apply the new requirements. There are possibilities that physical modifications will need to be made to facilities to deploy the necessary controls to restrict physical access. Additionally, to deploy a Low Impact Electronic Access Point, it is possible that certain systems or computer network architectures may need to be modified to accommodate the addition of an access point.
Yes
SMUD supports the removal of the IAC language from the 17 requirements and the continued work by NERC to develop the Reliability Assurance Initiative.
Yes
SMUD appreciates NERC's work on the development of the RSAWs related to CIP Version 5 and Revisions. SMUD is concerned that the RSAWs have not sufficiently incorporated the

specific language of the standards or the measures. It is unclear from reading the currently posted RSAWs how auditors will use the measures to inform the Compliance Assessment Approach.
Group
Arizona Public Service Company
Raymond Myford
Yes
Yes
Yes
Yes
Yes
Yes
No
Individual
Judy VanDeWoestyne
MidAmerican Energy Company
No
The revised structure of the CIP-003-6 is an improvement for the low requirements. However, some concerns remain. We find the new LERC definition needs clarification. Therefore we must vote no on the requirements that reference the definition. //Attachment 1, Element 2 - The placement of the phrase “based on need” with the commas in the statement may cause differences in interpretation. **Recommendation - Remove “based on need” from the requirement and the guidelines and technical basis because it is creating a more restrictive requirement for lows than for medium BES Cyber Assets that don’t have external routable connectivity. For those medium impact BES Cyber Assets, CIP-006-5 R1.1 requires entities to “restrict physical access,” without requiring ‘authorization’ or ‘based on need.’ // Attachment 1, Element 4 - Cyber incident response – 4.6 record retention was added with draft 2. It is unclear why. This is a ‘documentation only’ requirement and is duplicative to the record retention in Compliance Monitoring section C of every standard. **Recommendation – Remove this requirement. // Att. 1 – Element 4 Cyber incident response – 4.7 plan update. We find no support for the 180 day limit. Given the scale of lows, there could be multiple 180-

day clocks to track. While it's important to keep plans current, triggering updates for lows for discrete incidents is administratively burdensome compared to the risk. **Recommendation - At least once every 15 calendar months, review the Cyber Security Incident response plan(s) (unless the plan(s) have already been reviewed under CIP-008) and update, if needed. Note: We're concerned about double jeopardy for entities that leverage their COP-008 plan(s). // As with MidAmerican Energy Company's draft one comments, we recommend addressing dispersed generation with respect to the CIP-003-5 R2 requirements for low impact BES Cyber Systems. The dispersed generation SAR scope is to make it clear "what, if any, requirements should apply to dispersed generation … Unless this clarity is provided applicability at a finer level of granularity related to dispersed generation may be seen as required and such granularity will result in activities that have no benefit to reliable operation of the BES. Furthermore applicability at a finer level of granularity will result in unneeded and ineffective collection, analysis, and reporting activities that may result in a detriment to reliability." Standards under revision "should be examined and revised, as needed, to ensure it is clear that these activities and reporting are conducted at the point of aggregation to 75 MVA, and not at an individual turbine, inverter or unit level for dispersed generation." ** We recommend the CIP and dispersed generation drafting teams continue to collaborate to clarify the applicability of CIP-003-5 R2 for low impact BES Cyber Systems for dispersed generation. Where a Registered Entity can demonstrate that a dispersed generation low BES Cyber System cannot adversely impact 75MVA or more within 15 minutes, the R2 requirements should not apply to the dispersed generation low impact BES Cyber System. The burden of proof is on the Registered Entity. The requirements apply if the Registered Entity cannot meet the burden of proof. Appropriate text could be added to the R2 requirement.
No
The LERC definition is not clear. The second sentence uses undefined terms and refers to specific technologies, which over the time will make the definition obsolete as technologies change. The use of capital letters for Intelligent Electronic Device creates confusion by suggesting it is a glossary term. The exclusion is not present for medium or high impact. Explain the difference. // 'Background' in the 'Applicability' section for CIP version 5 of standards 004 through 007, includes the following: "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." Is this relevant for low impact BES Cyber Systems? If so, should it be included in CIP-003-6?
No
The revised structure of the CIP-010-2 and many of the revisions are an improvement for the transient devices requirements. However, some concerns remain. As with draft 1, use of the word 'Authorized' requires an additional level of documentation, which is more burdensome given the scale of low impact BES Cyber Systems. **Recommendation - Remove 'Authorized.' Entities would still be required to "specify" users, locations and use (individually or by group) for each part in Element 1.2 and 3.1 to meet the FERC directive. // Att. 1 – Element 2 Vendor/contractor owned or managed – 2.3 - The intent of this requirement is clear in the guidelines and technical basis, but not in the words of the requirement. The requirement could be interpreted such that Responsible Entities shall determine whether additional mitigation actions are necessary for any (and all) of the methods specified (listed) in 2.1 and

2.2, not just the ones that were selected. Clarification is needed in the requirement, not just in the guidelines and technical basis. // Guidelines and Technical Basis for R4 Att. 1 Element 1.1 - Insert “type” with references to devices. For example, “…pre-authorize an inventory of devices or device types; or authorize devices or device types at the time….”
Yes
No
The implementation plan requires physical access controls for lows by April 1, 2018. These controls are to be applied to LEAPs, which based on the implementation plan, aren’t required to be identified until September 1, 2018, with the electronic access controls. We propose making them both the same date – September 1, 2018, to minimize confusion. However, we would prefer to keep the dates staggered if synchronizing the dates would make the implementation date April 1, 2018, for both of them.
Yes
We support removal of the IAC language with the understanding that compliance exceptions and other elements of the Reliability Assurance Initiative will be implemented in all regions in January 2015.
Yes
MidAmerican Energy Company thanks the Standard Drafting Team for commitment of their time and expertise to the development of these CIP version 5 revisions.

Additional Comments

SPP RE

Bob Reynolds

1. For the requirements applicable to Low Impact assets, the Standard Drafting Team (SDT) changed the structure of CIP-003-6, Requirements R1 and R2 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-003-6 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: (1) The wording of element 2 (physical controls) has an issue – the phrase “based on need…” is misplaced and should be modified to appear earlier in the sentence. The SPP RE recommends the sentence be modified to read as follows: “Physical access controls: Each Responsible Entity shall, based on need as determined by the Responsible

Entity, implement controls to restrict physical access to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Low Impact BES Cyber System Electronic Access Point, if any, through one or more of the following:" (2) Element 4.6, which requires record retention related to Reportable Cyber Security Incidents, is nonsensical as written. The requirement should establish a minimum expectation; otherwise the Responsible Entity could declare a one-second retention period and the auditor would have no option except to find compliance. (3) Element 4.7, allowing 180 calendar days to update an incident response plan, is excessive and unreasonable. Updating the plan in the same time frame as that for High and Medium impact BES Cyber Systems is not unreasonable given the importance and the anticipated very broad application of the requirement. (4) The Guidelines and Technical Basis for Requirement R2 states that monitoring does not imply logging. At issue is how the Responsible Entity can demonstrate an effective monitoring process if unauthorized attempted or actual access is not recorded in some fashion.

2. The SDT proposed new definitions **Low Impact External Routable Connectivity** and **Low Impact BES Cyber System Electronic Access Point** to clarify the requirement language in CIP-003-6. Do you agree with the proposed new definitions? If not, please offer suggested revisions.

   Yes:

   No: X

   Comments: The SPP RE agrees with the definition of Low Impact External Routable Connectivity (LERC). SPP RE does not agree with the definition of Low Impact BES Cyber System Electronic Access Point (LEAP) with respect to the statement that allows the LEAP to be placed at an external location. This might not be an issue if the communication circuits between the LEAP and the protected BES Cyber Systems are private and managed by the Responsible Entity. When the communication circuits are over public Wide Area Networks using third-party service providers, placing the LEAP on the other side of the public network circuits provides minimal protection and exposes the protected assets to the risk of unauthorized access.

3. For the requirements applicable to transient devices, the SDT changed the structure of CIP-010-2, Requirement R4 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-010-2 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: (1) Element 1.4 should also include a requirement to ensure any removable media, such as a USB flash drive, is also externally scanned for malware before use with the Transient device. Element 3.2 implies such scanning is only necessary if the removable media is to be used with the BES Cyber System. (2) Any dependence upon the review of a

vendor policy or process, as permitted by Elements 2.1 and 2.2, needs to include a step to confirm the policy or process has been implemented for the transient device.

4. The SDT revised the proposed new definitions for Transient Cyber Assets and Removable Media to address issues raised in stakeholder comments. Do you agree with the proposed definitions? If not, please offer suggested revisions.

   Yes:

   No: X

   Comments: (1) The SPP RE again urges the Standards Drafting Team to eliminate the less than 30 day usage period found in the definition of Transient Cyber Asset, and require instead that the transient device be disconnected from the BES Cyber System or network immediately when its intended temporary use is complete and to remain disconnected until the next temporary use is required. Otherwise, a Responsible Entity could essentially maintain a routine, long-term network connection with only momentary connection breaks and thus bypass the security controls imposed on BES Cyber Assets that are normally connected for the long term. (2) The 30-days or less qualification in the Removable Media definition is unnecessary and may preclude the use of removable media containing authentication (e.g., digital certificates) or license (e.g., PSS/E dongle) information.

5. In response to stakeholder comments, the SDT revised the implementation deadlines. The implementation plan now includes tiered deadlines for the aspects of CIP-003-6. The CIP-007-6 timeframe is now consistent with CIP-006-6. Are these timeframes reasonable and appropriate? If not please explain specifically which implementation plan item needs adjusting and include the rationale for the suggested change.

   Yes: X

   No:

   Comments:

6. The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.

   In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

Yes: X

No:

Comments:

7. Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.

   Yes:

   No: X

   Comments:

Calpine Energy
Hamid Zakery

Calpine agrees with removing " identify, access, and correct" from the standards for High and Medium impact categories but recommend keeping " identify, access, and correct" for Low impact category.

Austin Energy
Thomas Standifur

1. For the requirements applicable to Low Impact assets, the Standard Drafting Team (SDT) changed the structure of CIP-003-6, Requirements R1 and R2 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-003-6 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: Recommend the requirements for physical security of low assets be deleted. This requirement is repetitive of safety requirements in the National Electrical Safety Code (NESC), Section 11 - Protective arrangements in electric supply stations, paragraph 110

General requirements. The NESC includes requirements to protect the public from high voltages. The safety aspects of the NESC are more stringent than the requirements in the proposed NERC standard and public safety is a higher concern than the less likely occurrence of security concerns at a low impact asset. Specifically the proposed CIP-003-6 requires:

The proposed NERC requirement allows technical physical security controls to restrict physical access to both. A fence with a locked gate, which is required by the NESC appears to meet the proposed NERC requirement to restrict physical access to both the asset and the cyber asset. The other suggestions in the draft standard could be provided in a best practices document. The requirement for physical security of low assets should be deleted.

2. The SDT proposed new definitions **Low Impact External Routable Connectivity** and **Low Impact BES Cyber System Electronic Access Point** to clarify the requirement language in CIP-003-6. Do you agree with the proposed new definitions? If not, please offer suggested revisions.

   Yes:

   No: X

   Comments: The LERC should specifically exclude communications aided relaying used for pilot relaying protection. Also, there is a high risk of confusion when using technical jargon in NERC definitions. Both of these definitions fall within this high level of confusion. If a national reliability standard requires too much technical jargon, it is written at the wrong level for its purpose. The reliability standard should be written to avoid the use of these definitions.

3. For the requirements applicable to transient devices, the SDT changed the structure of CIP-010-2, Requirement R4 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-010-2 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: While the language in the proposed requirements is a good practice, it creates significant compliance burden for entities to maintain documentation to prove compliance; plus, additional resources will be required to implement compliance controls that yield minimal risk reduction for the reliability of the BES. Transient devices will be a source of possible violations in future internal compliance reviews for self reports and also compliance audits. Section 1.2 of Attachment 1 is not needed and should be removed. Requirements already exist for anyone having access to protected cyber systems. Section 1.2 puts an entity in double jeopardy of violating multiple requirements for one action. The same comments apply to section 3.1 of attachment 1 and this requirement should be removed.

4. The SDT revised the proposed new definitions for Transient Cyber Assets and Removable Media to address issues raised in stakeholder comments. Do you agree with the proposed definitions? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

5. In response to stakeholder comments, the SDT revised the implementation deadlines. The implementation plan now includes tiered deadlines for the aspects of CIP-003-6. The CIP-007-6 timeframe is now consistent with CIP-006-6. Are these timeframes reasonable and appropriate? If not please explain specifically which implementation plan item needs adjusting and include the rationale for the suggested change.

   Yes:

   No:

   Comments:

6. The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.

   In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

   Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

   Yes:

   No: X

Comments: As stated in previous comments, we do not support the removal of the IAC language. Removal of the IAC language is a return to zero tolerance and RAI does not magically make a violation disappear. Our suggestion is to delete any requirement from the standard that contains IAC language. This is our opportunity as an industry to remove the sections, develop better language as FERC allowed, or face multiple violations of these zero tolerance requirements for many years. We've rushed through all the previous versions to meet a deadline. This is the time to work on a solution and get a better standard. We are working to meet compliance deadlines for version five standards while making changes to the standards – this can't be a good practice. FERC approved the version five standards; they didn't remand

them back. We have an official compliance date to meet for version five. Worse case, let's use the IAC language as currently approved.

7. Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.

   Yes: X

   No:

   Comments: The NERC CIP standards have resulted in numerous violations to registered entities and have been difficult to implement. These standards must get to a steady state and changes to the standards should be limited to an absolute minimum.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02
CIP Version 5 Revisions

Consideration of Comments
Additional Comment Period

November 25, 2014

RELIABILITY | ACCOUNTABILITY




Table of Contents

Consideration of Comments: Project 2014-02 CIP Version 5 Revisions

The Project 2014-02 Standard Drafting Team (SDT) thanks all commenters who submitted comments on the draft Critical Infrastructure Protection (CIP) Reliability Standards. These Reliability Standards were posted for a 45-day public comment period from September 3, 2014 through October 17, 2014. Stakeholders were asked to provide feedback on the Reliability Standards and associated documents through a special electronic comment form. There were 70 responses, including comments from approximately 164 different people from approximately 117 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

This consideration of comments is responding to the comments received on the standards and implementation plan balloted as CIP-003-6 and CIP-010-2 during the additional comment period and ballot. These standards included revisions to address the low impact and transient devices directives. There was a concurrent 45-day comment period and ballot of the Version X standards and implementation plan that addressed only the identify, assess, and correct (IAC) and communication networks directives. The SDT's responses to comments on those revisions are available here.

All comments submitted may be reviewed in their original format on the CIP Version 5 Revisions SDT project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, please contact Valerie Agnew, the Director of Standards, at 404-446-2566 or valerie.agnew@nerc.net. There is also a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process can be found in the Standard Processes Manual.
http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Introduction

The SDT appreciates industry comments on the revisions to the CIP Reliability Standards. During the development of the revised standards prior to posting, the SDT made it a priority to conduct outreach as modifications were made to the standards. The SDT conducted three face-to-face meetings to revise the standards, Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs) in order to appropriately consider all comments received. The SDT continued its rigorous conference call schedule as it understands the importance of getting these standards to steady state.

Background

On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards and also directed that NERC make the following modifications to those standards:

1. Modify or remove the "identify, assess, and correct" (IAC) language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for to assets containing low impact BES Cyber Systems.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the IAC language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the low impact and transient electronic devices directives. The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.

Question 1: CIP-003-6

1. *For the requirements applicable to Low Impact assets, the Standard Drafting Team (SDT) changed the structure of CIP-003-6, Requirements R1 and R2 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-003-6 Attachment 1? If not, please explain your objections and offer suggested revisions.*

Placement

Several stakeholders commented on the placement of the low impact requirements in the CIP suite of standards. Tennessee Valley Authority (TVA), New York Power Authority, and Iberdrola USA commented that they preferred the low impact requirements in the relevant CIP standard rather than as a plan in CIP-003. American Electric Power (AEP) and Independent Electricity System Operator (IESO) suggested the SDT place the requirements in a table format similar to other CIP standards. However, Exelon, Edison Electric Institute (EEI), Southern Companies, MidAmerican Energy Company, NV Energy, Consumers Energy Company, FirstEnergy, Colorado Springs Utilities, Occidental Chemical Corporation, Pepco Holdings, Sacramento Municipal Utility District (SMUD), Bonneville Power Administration (BPA), and ACES Standards Collaborators expressed support for the current CIP-003 plan structure for low impact requirements.

The SDT appreciates the comments regarding the placement of the low impact requirements and determined to retain the current CIP-003 plan structure due to a majority of stakeholder support.

Attachment 1

Several commenters suggested revisions to the sections included in Attachment 1 to CIP-003-6, Requirement R2. Please note that the SDT changed the term "element" to "section" in response to several comments so the remainder of this document will use "section" even if commenters referred to "element."

For section 1, NIPSCO, EEI, Oncor Electric Delivery Company LLC, Iberdrola USA, NV Energy, FirstEnergy, and Pepco Holdings suggested that the SDT make Attachment 1 language consistent with Attachment 2 by using "through one or more of the following" and labeling Attachment 1 sections similar to Attachment 2. Dominion also commented that Attachment 1 should be consistent with Attachment 2. Exelon suggested that the SDT relocate the bullets from the requirement in Attachment 1 to the measures in Attachment 2. Exelon further commented that the SDT should remove "its" because it is more prescriptive than CIP-004-6, Requirement R1. Massachusetts Municipal Wholesale Electric Company (MMWEC), Colorado Springs Utilities, Indiana Municipal Power Agency (IMPA), SMUD, BPA, and Florida Municipal Power Agency (FMPA) recommended changing "once every 15 calendar months" to "at least once every 15 calendar months." In response to these comments, the SDT changed the word "element" to "section" throughout the standard, moved the bullets from the requirements language to the measures, removed "its" as suggested, and revised the requirement to read "at least once every 15 calendar months."

For section 2, Dominion, MMWEC, MidAmerican Energy Company, MRO NERC Standards Review Forum, and Luminant Generation Company commented that "based on need" should be removed. SPP-RE commented that the phrase "based on need" should be moved to earlier in the sentence. Dominion, NIPSCO, EEI, Oncor, Southern Companies, Iberdrola USA, NV Energy, FirstEnergy, Pepco Holdings, SMUD, BPA, and IMPA recommended that the SDT ensure that the terms for physical controls are consistent between attachments and suggested using the term "physical security controls."

The SDT revised CIP-003-6, section 2 to clarify that the Responsible Entity is obligated to "control physical access" at the asset or location containing the low impact BES Cyber System. The SDT moved, but retained, the phrase "based on need" so that criteria are established by which to control access. The need for access is to be

"determined by the Responsible Entity" to accommodate facts and circumstances relevant to the location. This revision addresses the FERC Order No. 791 directive to add objective criteria or specificity to the requirement.

Note, in response to other comments, the SDT changed "access" to "security" and "to restrict" to "control" and made the suggested change to "physical security controls."

Dynegy suggested that the SDT use "or" rather than "and" in section 2 and commented that an inventory is required if the language used "and." The SDT appreciates the comment. The SDT used "and" to restrict access to both the asset/location of the BES Cyber System and the LEAP should it reside outside of the asset/location. Entities would need to physically protect two spots if they were separate. The graphics in the guidance shows this scenario for electronic access. If the LEAP is located within the asset containing the low impact BES Cyber System, the entity would need to show how the asset containing both the LEAP and the low impact BES Cyber System is protected. It is still one obligation to show how physical access controls are being applied to either item. The intent of the language is for an entity to have an inventory of the LEAPs, but not inventories of low impact BES Cyber System(s) and their individual Cyber Assets.

Nebraska Public Power District (NPPD) recommended that section 2 requirements for physical security be deleted and the vulnerabilities are covered by national Electrical Safety Code, Section 11. The SDT thanks you for the comments. CIP-003-5 incorporated physical security obligations for assets/locations with low impact BES Cyber Systems into the suite of requirements under the NERC purview. FERC approval of CIP V5 and the Order No. 791 directives obligate the drafting team to retain the physical security requirements.

AEP and Xcel Energy commented that section 2 is more prescriptive than medium impact without External Routable Connectivity and would be a compliance burden. The SDT revised CIP-003, section 2, and removed some of the specific list of physical security controls. Section 2 retains "based on need" as a qualifier to physical security controls, but it's used to make the section objective clear.

For section 3, TVA commented that establishing a LEAP assumes an ESP which is subject to CIP-005-5, Requirement R1 with inbound and outbound access subject to CIP-007-6, Requirement R1. The SDT thanks you for your comment. The requirements for low impact BES Cyber Systems are contained solely within CIP-003-6, R2. No other CIP standards related to high and medium impact BES Cyber Systems apply.

EEI, Oncor, Southern Companies, Iberdrola USA, FirstEnergy, Pepco Holdings, SMUD, BPA, IMPA, Entergy Services, and American Public Power Association (APPA) commented that the LERC and LEAP acronyms were missing from sections 2 and 3. The SDT added the acronyms where appropriate in the requirement.

For section 4, Dominion, CenterPoint Energy Houston Electric, EEI, NIPSCO, Oncor, Southern Companies, Iberdrola USA, NV Energy, Consumers Energy Company, Xcel Energy, MRO NERC Standards Review Forum, FirstEnergy, Pepco Holdings, and Luminant Generation Company suggested that the SDT add "if needed" to the requirement to update the Cyber Security Incident response plan(s). Exelon requested that the SDT clarify the intent of the phrase "either by asset or groups of assets" to confirm whether enterprise-wide plans could fulfill the obligations. Exelon, MidAmerican, and NRECA requested that the SDT justify the addition of 4.6 and 4.7 and the 180-day clock because it could cause entities to maintain multiple clocks for different impact levels. SPP-RE commented that the record retention requirement in Section 4.6 does not make sense and recommended that the requirement establish a minimum expectation. SPP-RE further commented that the updates for Section 4.7 take place at the same frequency as that of medium and high impact BES Cyber Systems.

The SDT confirms that the phrase "either by asset or by groups of assets" accommodates use of an enterprise-wide plan for multiple assets or locations to fulfill the obligation. The SDT added language to the guidelines to emphasize the point. The SDT removed 4.6; however, retained 4.7. The SDT finds the updating of the Cyber

Security Incident response plan following a test or actual Reportable Cyber Security Incident to be a valuable security step, if updates are needed. The SDT added "if needed" in recognition that updates may not always be needed. The SDT retained the "180 calendar days" time period for updates. This is a reasonable amount of time to make updates. Entities may make the updates sooner ("within 180 calendar days") if preferable for their program.

MMWEC suggested changing identification, classification, and response to Cyber Security Incidents to identification and classification because response is a subset of incident handling. In addition, MMWEC commented that because the testing is every 36 months, entities should be required to ensure individuals are aware of their response roles through more frequent training or review their responsibilities. Consider review roles at least once every 15 calendar months. The SDT thanks you for your comments. In the initial comments, stakeholders preferred a closer alignment between the CIP-008 and the CIP-003 elements to help accommodate entities that will have multiple impact levels. Given the risk, the SDT thinks 36 months is appropriate.

Northeast Power Coordinating Council (NPCC) requested clarification where dividing line is between section 4 and EOP-004. The SDT notes that EOP-004-2 does not cover the reporting of Cyber Security Incidents. Entities may choose to use the same plan used for EOP-004-2 for Reportable Cyber Security Incidents.

Lincoln Electric System and Consumers Energy Company commented that section 4 is virtually identical to CIP-008-5 for medium and high impact BES Cyber Systems and noted that the requirement would be burdensome for low impact without External Routable Connectivity. The SDT removed 4.6 to reduce the burden. The requirement allows Responsible Entities to use an enterprise Cyber Security Incident response plan and not develop individual by asset or device to also reduce the burden.

Texas Reliability Entity (TRE) recommended that additional elements be added to CIP-003 regarding low impact to reduce the risk to high and medium impact assets: information protection, recovery functions, system security functions, and configuration change management. The SDT thanks you for the comments. The SDT considers the controls for low impact BES Cyber Systems to be appropriate to their level of risk to the Bulk Electric System.

Entergy Services suggested that the SDT align the electronic access controls with the physical access controls to provide entities latitude. The SDT thanks you for the comments. The SDT considers the controls for low impact BES Cyber Systems to be appropriate to their level of risk to the Bulk Electric System.

Exelon expressed support of the standalone nature of the requirements in sections 2 and 3 and states they are consistent with medium and high impact requirements but tailored to lows. The SDT thanks you for the comment.

Kansas City Power and Light and BC Hydro commented that the protections are too detailed and excessive and represent too large a pool of assets that do not have a substantive impact to the Bulk Electric System. The SDT thanks you for the comments. The SDT considers the controls for low impact BES Cyber Systems to be appropriate to their level of risk on the Bulk Electric System.

Attachment 2

TVA commented that Attachment 2 does not offer much clarity beyond what is already documented in Attachment 1 and examples of evidence should be documented in table format. The SDT thanks you for your comments but notes that it received support of the details outlined in Attachment 2.

Dominion, NIPSCO, EEI, Oncor, Southern Companies, Iberdrola USA, Xcel Energy, SMUD, BPA, APPA, and IMPA commented that section 2 of Attachment 2 did not include "perimeter controls" like the guidelines and suggested section 2 include it. The SDT added "perimeter controls" to Attachment 2 as recommended.

MMWEC suggested that the SDT change "(e.g. IP addresses, ports, services) to "(e.g. by restricting IP addresses, ports, and/or services)" and to move the phrase following "deems necessary." The SDT added the text "(e.g. by restricting IP addresses, ports and/or services)" as recommended.

List of Assets

TVA commented that the CIP-003-6 Guidelines that say "using the list of assets from CIP-002" contradicts CIP-002-5.1, Requirement R1, Part 1.3 which states "a discrete list of low impact BES Cyber Systems is not required." Exelon Companies, Idaho Power, Xcel Energy, and NRECA requested the SDT to discuss how to demonstrate compliance without a list of Systems and suggested the SDT add guidance on the note in the requirement.

The SDT notes that the list of assets containing low impact BES Cyber Systems from CIP-002-5.1 ("Part 1.3 list") is different from a discrete inventory of low impact BES Cyber Systems and the Cyber Assets that make up the low impact BES Cyber System ("cyber list"). The Part 1.3 list of generation plants, substations, control centers, etc. must be maintained and provided at audit. The cyber list; however, is not required. A cyber list would encompass every Cyber Asset in every BES asset across the NERC region. The SDT determined and FERC supports in Order 791, the effort to flawlessly maintain the cyber list over the audit period at each BES asset does not match the level of risk.

The items in CIP-003-6 Attachment 1 were written to be assessed at a physical asset containing low impact BES Cyber System(s) site level. The cyber security policies, awareness program, and incident response plan can be assessed through the assessment of the documented processes. The physical security controls can be assessed at the site level. The electronic access controls were developed to focus protection on the presence of Low Impact External Routable Connectivity (LERC) and establishing boundary protection with LEAP(s), if any. It is intended that entities will have an inventory of LEAPs, if any, but not a cyber list of the individual low impact BES Cyber System(s) Cyber Assets. An assessment may spot-check an asset containing low impact BES Cyber System(s) site to determine whether the cyber security plan(s) meets the objectives of the physical security controls at the asset containing the low impact BES Cyber Systems and whether LERC exists and LEAPs are properly established. However, a Cyber List of the low impact BES Cyber System(s) or their associated Cyber Assets is not required to perform this assessment.

Other

TVA commented that the Violation Severity Levels (VSLs) for CIP-003, Requirement R2 are in the Severe category but apply to low impact systems. The SDT notes that VSLs do not measure risk but the level of violation of the requirement. The VSL construct indicates that a binary VSL would use the Severe column. In addition, the VRF assesses risk, and the requirement's VRF is Lower.

TRE recommended replacing "its" with "a Responsible Entity's" in the Rationale of Requirement R1. The SDT replaced "its" with "a Responsible Entity's" per the recommendation.

Lincoln Electric System recommended replacing the term Bulk-Power System with Bulk Electric System in the Rationale of Requirement R2. The SDT replaced Bulk-Power System with Bulk Electric System as recommended.

Dominion suggested revising the Requirement R2 guidance to state, "The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do still meet the definition of having a 15-minute adverse impact so some protections are needed." Dominion also suggested revising the guidance to state, "Low Impact BES Cyber System Electronic Access Point (LEAP) – a Cyber Asset interface that allows Low Impact External Routable Connectivity." The SDT revised the sentences but retained the concepts.

NIPSCO, EEI, Oncor, Iberdrola USA, AEP, and Pepco Holdings recommended removing the sentence that states, "Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised" because aggregating low impact BES Cyber Systems across multiple sites does not reflect a true risk-based assessment and therefore this sentence is not accurate. The SDT removed the sentence form the Rationale for Requirement R2.

NIPSCO, EEI, Oncor, Iberdrola USA, and Pepco Holdings commented that the bold subtitles in the Guidelines are inconsistent with section language in Attachment 1 and recommended changing the titles for Cyber Security Awareness and Physical Security Controls. The SDT revised the titles accordingly.

Exelon suggested that the SDT consider using "require" or "obligate" rather than "imply" in the guidance on Requirement R1, Attachment 1 – Physical Security and suggested making LEAP plural in the same section. The SDT revised the language to say "require." The SDT thanks the commenter for the suggestion to make LEAP plural but ultimately removed the language.

Southern Companies commented that the scenario for LERC and LEAP in the Attachment 2 Guidelines is unclear as to which firewall is the LEAP and suggested adding a scenario where there is LERC and an entity has flexibility to determine the LEAP. The SDT added additional scenarios to the Guidelines to clarify LERC and LEAP.

Southern Companies also suggested that the SDT rephrase the Guidelines to state, "However, the LERC between assets 'behind' the LEAP must pass through the single LEAP." The SDT revised the language accordingly.

Southern Companies, SMUD, BPA, IMPA, and APPA commented that the SDT should revise the Guidelines regarding EACMS and LEAPs and suggested that the SDT create a paragraph stating, "However, a LEAP can be implemented within the same Cyber Asset that is serving the function of EACMS or EAP for a medium or high impact BES Cyber System. This is possible because a LEAP is the interface on the controlling Cyber Asset (e.g. firewall or router) and not the Cyber Asset itself." The SDT addressed EACMS in the context of LEAPs in the Guidelines.

SPP-RE commented that the Guidelines for Requirement R2 states that monitoring does not imply logging and questioned how a Responsible Entity can demonstrate effective monitoring without recording unauthorized access or attempts at access. In response, the SDT notes that monitoring includes human observation or alerting mechanisms, and the retention of access logs is not required to implement monitoring controls.

Luminant Generation Company suggested several revisions to the Guidelines. For the Guidelines on Requirement R2, Attachment 1, Luminant commented that a discussion on LERC was not clear and recommended revisions to state, "SDT intends IED to IED communications be exempt from any requirement to use an LEAP even if there is LERC. Through this exemption, the SDT intends to not preclude the use of time-sensitive reliability enhancing data exchanges." In response, the SDT revised the LERC definition for clarity. Luminant suggested that the SDT revise the sentence regarding LEAPs and EACMS to read, "A LEAP is not to be considered an EACMS. In response, the SDT developed additional guidance regarding LEAPs and EACMS. Luminant suggested that the SDT replace "interface" with "internal interface" in the Guidelines describing LEAP. The SDT appreciates the comment but retains the language to better convey the practical use of interface in the definition. Luminant also suggested revising the Guidelines on LEAP to state, "…must also pass through a LEAP" instead of "must also pass through the single LEAP." Furthermore, Luminant suggested deleting "physically" from "unidirectional gateway that physically enforces outbound-only data flows." For the sentence beginning "The electronic access controls," Luminant suggested that the SDT replace shall with should. Finally, Luminant suggested that the SDT delete the sentence regarding assets without LERC and real-time monitoring. The SDT revised the language according to these suggestions but removed "unidirectional gateway."

Hydro-Quebec commented that the compliance date for electronic access controls is after the date for physical security controls in the Implementation Plan. The SDT has modified the Implementation Plan to make the compliance date for electronic access and physical security controls consistent.

MidAmerican and PacifiCorp recommended that the SDT continue working with the drafting team regarding dispersed generation applicability to determine what, if any, requirements apply to dispersed generation. The CIP SDT will continue to collaborate with the DGR SDT to address concerns with CIP and DGR.

Exelon, NYPA, Seattle City Light, MidAmerican, SMUD, BPA, IMPA, and APPA expressed concern that in a multi-impact rated program any failure to fulfill a requirement such as those in Sections 1 and 4 in Attachment 1 could result in violation of CIP-004 and CIP-008 as well. The SDT collaborated with NERC Enforcement in response. Responsible Entities may choose to implement multi-impact rated programs to address low, medium, and high impact BES Cyber Systems. It is possible the same facts and circumstances may indicate noncompliance of both the requirements applicable to low impact BES Cyber Systems and the corresponding requirements applicable to high and medium impact BES Cyber Systems. That the same act or omission may result in two separate violations is not unique to the CIP V5 standards. For example, the same failure to act immediately could constitute a violation of both TOP-001-1a R2 and TOP-008-1 R1. NERC's *Sanction Guidelines* provide that one penalty may be assessed where there are multiple violations arising from a single act or common incidence of noncompliance. Therefore, if a penalty is assessed at all, it would not be duplicated. In addition, the disposition of any noncompliance is based on the level of risk posed to the reliability of the BPS. Therefore, in the event one or more of the instances of noncompliance poses a minimal risk, a number of streamlined options is available, including treatment as a compliance exception. As with any noncompliance, a determination of whether compliance exception treatment will be appropriate in a given case will depend on the facts and circumstances.

Question 2: Low Impact Definitions

2. *The SDT proposed new definitions Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) to clarify the requirement language in CIP-003-6. Do you agree with the proposed new definitions? If not, please offer suggested revisions.*

LERC in DMZ

TVA, EEI, NIPSCO, Oncor, Iberdrola USA, and FirstEnergy requested clarity regarding the scenarios in the Guidelines, specifically where the LEAP is located in the diagram and when LERC exists. TVA commented that it is unclear whether LERC exists in a scenario where all external communication is through a jump host or historian in a demilitarized zone (DMZ). The SDT added additional diagrams to the Guidelines and modified the definition to provide more clarity regarding LERC. The new definition states LERC is "*direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s)….*"

In the Guidelines, it clearly demonstrates that if all communication from the low impact BES Cyber Systems is internal (e.g. the DMZ is implemented in such a way to restrict all external communication to the BES Cyber System), then LERC does not exist. In this case, the objective of protecting the low impact BES Cyber System is achieved.

Be aware, however, that if the low impact BES Cyber System has established bi-directional routable communication to an external Cyber Asset, then LERC does exist. This would be the case even if the low impact BES Cyber System communicates through a jump host DMZ using the same protocol session with an external Cyber Asset.

LEAP "Allows"

TVA, EEI, NIPSCO, NV Energy, Oncor, Southern Companies, Iberdrola USA, FirstEnergy, MRO NERC Standards Review Forum, and SMUD commented that the term "allows" in the definition is too broad and suggested that the SDT consider "controls" or "restricts." Duke Energy suggested using "permits." NPCC and NYPA commented that the guidance states "allows and controls" whereas the definition states "allows." The SDT agrees there is an inconsistency and changed "allows" to "controls" in both the definition and the guidance.

61850 Exclusion

Several stakeholders commented on the exclusion included in the LERC definition. Dominion, EEI, NIPSCO, NV Energy, Oncor, Southern Co, Iberdrola USA, and FirstEnergy requested clarification in the guidance that LERC excludes "point to point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time-sensitive protection or control functions." PacifiCorp and MidAmerican commented that the exclusion used undefined terms that cause confusion and refer to specific technologies which may become obsolete over time. In addition, PacifiCorp and MidAmerican commented that the exception seems to remove protections indiscriminately rather than addressing the assets to be protected. MidAmerican further commented that the use of capital letters for Intelligent Electronic Device creates confusion because it is not a defined NERC Glossary term and requested that the SDT explain why there is no exclusion for medium or high impact assets. NPPD commented that LERC should specifically exclude communications aiding in relaying used for pilot relaying protection and that the definition should be written to avoid technical terms. Pepco Holdings requested additional guidance on the exclusion.

The SDT revised the exclusion according to the suggestion to use "point to point communications…." The SDT coordinated with protection engineers to ensure the language was clear as to the exclusion. The SDT also put intelligent electronic device into lower case letters. The SDT considered removing the technologies in the

parentheses but determined that the examples provided clarity for some stakeholders. The SDT reviewed the language to limit technical terms as necessary and ultimately determined that the revisions made to the definition provide as much detail as necessary to reflect the SDT's intent. The SDT considered guidance related to the definition but determined that guidance would not be helpful because the terms would be moved to the NERC Glossary where there is no associated guidance. Therefore, the SDT focused on including detail in the definition rather than explanations in the guidance. Regarding the lack of exclusion for medium and high impact, the SDT considered this exclusion appropriate for low impact BES Cyber Systems because of the lower level of risk and large scale of applicability. The SDT explains the rationale for the exclusion in guidance stating the intent not to require a LEAP even though there is LERC or to preclude the use of such time-sensitive reliability enhancing functions if they use a bi-directional routable protocol.

Acronyms

EEI, NIPSCO, Oncor, Iberdrola USA, and FirstEnergy suggested that the SDT use the LEAP and LERC acronyms throughout the standard. The SDT agrees and added the acronyms in the definition and throughout the standard.

LEAP and EACMS

Several stakeholders commented on the relationship between LEAP and Electronic Access Control or Monitoring System (EACMS). EEI, NIPSCO, Duke Energy, Iberdrola USA, FirstEnergy, and FMPA commented that the definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the LEAP rather than the device containing the NIC and that it is possible to have a NIC port inside a high or medium impact BES Cyber System Electronic Security Perimeter (ESP) in an EACMS. The commenters recommended additional guidance on the relationship between the LEAP and EACMS. TRE recommended removing the last sentence of the LEAP definition regarding EACMS.

The SDT removed the sentence "The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System." The SDT also revised the guidance to address the relationship between LEAP and EACMS.

BPA commented that using the term "access point" in LEAP creates confusion with medium and high impact EAP. The SDT thanks you for your comment. The SDT determined that the similar concepts from the medium and high impact EAP assisted entities in understanding expectations. However, the SDT revised the definition in response to comments to improve clarity.

Other

Entergy Services commented that it disagrees with the application of acronyms to only low impact. The SDT discussed the trade-offs of developing and applying a definition to only one standard. While not ideal to create definitions used in one standard, it resolved many clarity concerns the SDT had with the requirement language. The SDT decided that clarifying the terms used in the requirement language was beneficial.

MMWEC commented that "low impact BES Cyber System" should be "BES Cyber Systems associated with Low Impact assets" and that the SDT should consider changing "communication protocols created" to "communication using protocols created." The SDT thanks you for your comments. In the CIP-002-5 categorization, entities categorize the assets containing low impact BES Cyber Systems. The term low impact assets is not used. The phrase "communication protocols created…" has been replaced.

IESO commented that the definition for LERC states that "Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s)" and suggested that the statement should include both BES Cyber Systems and BES Cyber Assets as LERC should apply to both systems and assets. The SDT thanks you for the comment. Per the definition, a BES Cyber System is

one or more BES Cyber Assets and every BES Cyber Asset must be in one or more BES Cyber System(s); therefore it is a superset and includes both.

AEP commented that the definitions create confusion where they refer to "asset" when it appears the term should be "facility" and suggested changing the second lowercase use of the word "asset" in each definition to be "facility." The SDT thanks you for your comment. The SDT previously considered the term “facility” but this term in lower case creates other challenges. The SDT selected “assets” to be consistent with CIP-002, which cites “assets” containing low impact BES Cyber Systems.

MidAmerican asked whether the Background in the Applicability section of CIP-003 should include the following phrase in the Background section of other CIP standards: “This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.” The SDT thanks you for your comment. The Background for CIP-003 is different from that within CIP-004 though -007 because low impact BES Cyber Systems are distinguished from high and medium impact BES Cyber Systems. This is not relevant for CIP-003-7 because the external routable connectivity is not used in reference to applicability.

Xcel Energy requested clarification on whether the logical network protected by the LEAP extends beyond a physical boundary and on whether the LERC definition is referring to access to or from a system or network. The SDT confirms the logical network protected by the LEAP may extend beyond a physical boundary. The SDT also confirms that designation of a LEAP does not imply additional obligations such as those for EACMS associated with medium or high impact BES Cyber Systems. All obligations for low impact BES Cyber Systems are found in CIP-003-7, Requirement R2.

Kansas City Power and Light (KCPL) and SPP and specific members commented that the new definitions are not clear. They commented that entities should describe their connectivity to their assets and how that’s managed. The SDT attempted many iterations of requirement language before defining the new terms. Use of the terms within the requirement language streamlined the requirement language and made it much clearer to understand the requirement obligations. Clearer requirement language reduces the risk of contradictory interpretations.

Encari requested clarification on the LERC definition and external connectivity and suggested “outside the network” instead of “outside the asset.” The SDT thanks you for your comment. The phrase “outside the asset” is intentionally used to keep the level of control at the asset/location level, but to accommodate the scenario in which a LEAP is located outside of the asset containing low impact BES Cyber Systems. The definition is not making a demarcation at the system level.

SPP-RE commented that it does not agree with the definition of LEAP because a LEAP may be placed external to the asset. Specifically, SPP-RE commented that protected assets could be exposed to the risk of unauthorized access if the communication circuits are over public Wide Area Networks using third-party service providers. In response, the SDT notes that a LEAP may be placed external to the asset, but all LERC must still be protected by a LEAP. The allowance of having an external LEAP does not provide the opportunity of having a Cyber Asset with unrestricted access to the low impact BES Cyber System. In addition, a LEAP must have physical security controls according to Section 2.

SPP-RE agreed with the definition of LERC. The SDT thanks you for your support.

Question 3: Transient Devices

3. *For the requirements applicable to transient devices, the SDT changed the structure of CIP-010-2, Requirement R4 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-010-2 Attachment 1? If not, please explain your objections and offer suggested revisions.*

Transient Cyber Assets Managed by the Responsible Entity

KCPL, SPP and specific members, and NPPD commented that Attachment 1, Section 1.2 contains requirements covered in other standards and should be removed. The SDT appreciates the comments received. However, the authorization in Element 1.2 is needed to identify who is specifically allowed to use these devices. The SDT agrees that these users may be a subset of the CIP-004-6 authorized users but contends that not all users will be listed in a program, (e.g., medium impact BES Cyber Systems without External Routable Connectivity does not require CIP-004-6 authorizations). Furthermore, CIP-004-6 requires authorization of the individual, whereas CIP-010 section 1.2 allows flexibility to document by individual or group. In response to your comment, the SDT revised the guidance for improved consistency.

AEP commented that section 1.2 regarding authorization of users is not practical when Transient Cyber Assets do not have External Routable Connectivity. The SDT appreciates the comment. However, the SDT considers authorization of users, regardless of External Routable Connectivity, to be necessary to address the risks posed by Transient Cyber Assets.

Luminant commented that section 1.3 "live operating system and software executable only from read-only media" is not clear. The SDT appreciates the comment. However, the SDT considers the current language to be in alignment with the intent of the requirement and technology available. Further, the SDT has concerns with Luminant's recommendation related to "other required executables". "Required" could introduce additional documentation elements that would be difficult to sustain. Additionally, Luminant suggested that the SDT should revise the section title for sections 1.4 and 1.5 to include "prevention" and recommended changing the requirement to include prevention and mitigation "if necessary." The SDT appreciates the comment. However, the SDT considers the title to be appropriate in defining the expectations and in line with the structure of the other elements. The SDT avoided using the term "prevent" to emphasize mitigation efforts over potential compliance concerns with a 100% performance standard that could be associated with "prevent". With regards to the addition of "if necessary" making the addition would further confuse the required actions.

SPP-RE commented that Section 1.4 should include a requirement to ensure any Removable Media is externally scanned for malware before use with a transient device. The SDT appreciates the comment. Scanning of Removable Media on the Transient Cyber Asset is not prohibited. The malicious code mitigation methods used by the Transient Cyber Asset could suffice in meeting this objective. Additionally, the SDT revised 3.2 to clarify that methods to detect malicious code on Removable Media are to be used on a Cyber Asset other than a BES Cyber System or Protected Cyber Asset.

Southern Companies suggested revising section 1.5 to state "The Transient Cyber Asset must reside within a location with restricted physical access." The SDT appreciates the comment. The SDT revised the language to read "Restrict physical access."

Transient Cyber Assets Managed by a Party Other than the Responsible Entity

Dominion and NPCC suggested revising sections 2.1 and 2.2 to state "at least one." The SDT appreciates the comments received. However, the language currently obligates an entity to use "at least one" through the requirement to "or a combination of" methods. The SDT made additional revisions to clarify the requirements.

Dominion commented that the "per Transient Cyber Asset capability" should be added to section 2.2. The SDT agrees with the comment and has revised the Requirement to address this concern.

SPP-RE commented that the review of a policy or process outlined in Sections 2.1 and 2.2 needs to include a step to confirm that the policy or process has been implemented for the transient devices. The SDT appreciates the comment. The entity is obligated to meet the objective of the requirement to mitigate the risk of software vulnerabilities and malicious code and demonstrate how this was accomplished for parties other than Responsible Entities. The SDT considers these appropriate controls for Transient Cyber Assets managed by a party other than the Responsible Entity in cases where complete verification may not be possible.

BC Hydro recommended that the SDT revise the requirements applicable to Responsible Entities regarding devices owned or managed by other entities because it would be infeasible to monitor other parties' devices. The SDT used the concept of a "plan" to allow the entity to define the controls and processes that are most appropriate to their organization. This includes determining how the entity will handle devices not under their management with the objective of meeting the performance requirements in Attachment 1, Section 2. Options are provided to enable the entity to be successful in protecting their systems from devices managed by parties other the Responsible Entity.

Exelon asked whether contract obligations could fulfill section 2. The SDT's response is yes, and further details are included in the Guidelines. To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department Of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [2] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

NPCC suggested adding authorization of vendor or contractor use of Transient Cyber Assets to section 1.2. The SDT appreciates the comment. The intent was not to require the entity to document vendor or contractor managed devices in the same manner as their own assets. However, entities should note that they need to demonstrate that the contractually obligated process was followed.

EEI, NIPSCO, Southern Companies, SMUD, MidAmerican, MISO, NPCC, and Iberdrola USA suggested adding "if necessary" to section 2.3 to clarify that entities can accept the device without requiring modifications. The SDT agrees with the comment, but opted to use "any" rather than "if necessary" for sentence structure.

CenterPoint recommended revising section 2.2 to read "...operating system software and other required executables *installed* from read-only media." The SDT appreciates the comment. However, the current language

[2] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

does not include the obligation to determine what is "required" to be installed on the device. It is simply to require all software, including the operating system be on read-only media.

AEP commented that section 2 should be removed because vendors and contractors are not subject to CIP requirements. The SDT appreciates the comments received and recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to protect against the introduction of malicious code on their BES Cyber Systems. The SDT used the concept of a "plan" to allow the entity to define the controls and processes that are most appropriate to their organization. This includes determining how the entity will handle devices not under their management with the objective of meeting the performance requirements in Attachment 1, Section 2. Options are provided to enable the entity to be successful in protecting their systems from devices managed by parties other than the Responsible Entity.

Removable Media

EEI and CenterPoint commented that Section 3.2 does not require the entity to take any action other than scanning Removable Media. The SDT agrees with the comment and revised the CIP-010, Attachment 1, Section 3.2 to address this concern.

EEI, AEP, and CenterPoint commented that Section 3.2 should be revised because it presumes that scanning takes place on an external system when technology exists on USB drives, for example, to do scanning. The SDT appreciates the comments received. The SDT extensively discussed and revised Section 3.2 to clarify the obligations. The language seeks to address the risks of scanning for malicious code on the BES Cyber Asset and to prevent introduction of malicious code on the BES Cyber Asset. While the requirement does not address virus scanning on USB drives specifically, it does not preclude the use either since it is external to the BES Cyber Asset. Evidence could include documentation of the implementation of antivirus on the scanning system or procedural documentation of the actions taken. The methods used by the entity should be addressed in the plan document(s). The Guidelines and Technical Basis has been modified to address this matter.

Exelon asked how often entities should scan Removable Media to fulfill Section 3.2. The SDT revised the Guidelines to address this concern.

TVA commented that it is not necessary that a user of an authorized Removable Media device have electronic access to the applicable system because an individual with physical access to a system could be connecting removable media for someone with electronic access but working remotely. The SDT appreciates the comment. To clarify, the entity is required to include in their plan authorization of those using the Transient Cyber Asset or Removable Media to connect to a BES Cyber System. References to CIP-004 authorizations within the guidance have been updated.

BC Hydro commented that Section 3 should be revised to provide clarity regarding authorized users. The SDT extensively discussed Section 3 and revised the Guidelines and Technical Basis.

Measures & Guidance

EEI, NIPSCO, SMUD, Southern Companies, MISO, and MidAmerican requested that the Guidelines address authorization based on a group of assets. The SDT revised the Guidelines and Technical Basis to address this concern.

EEI and NIPSCO recommended that the SDT remove the restatement of requirement language from the Attachment 2 as it is not an example of evidence. The SDT thanks you for and agrees with the comment and revised Attachment 2 to address this concern.

NIPSCO, Southern Companies, and NV Energy commented that Section 3.2 of Attachment 2 should include examples of capabilities or embedded, real-time virus scanning and encryption on USB drives. The SDT appreciates the comment and revised Attachment 2 to address this concern.

Luminant recommended removing the last sentence of the measures for Sections 1.3, 1.4, 1.5, 2.1 and 2.2. The SDT thanks you for the comment; however, the team considers the last sentence to be support of "per Transient Cyber Asset capability" noted in the section.

TRE recommended adding the following language to M4: "including but not limited to a list of in-scope transient devices, and manual or automated logs showing connection periods...." The SDT thanks you for your comment. The use of these devices is limited to the context of change management and vulnerability assessment. The use of a plan to document how the entity implements the requirement should be the sole evaluation criteria for consideration in determining and proving compliance.

ACES Standards Collaborators requested the SDT develop additional guidance regarding what is not considered a transient device. The SDT thanks you for your comment but notes that prior comments requested that guidance on "what is not a transient device" be removed. It is not feasible to note all of the possibilities of what could be included in this list.

EEI, NIPSCO, Southern Companies, FMPA, IMPA, and AEP requested guidance that mitigation does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system. The SDT thanks you for and agrees with the comment and revised the Guidelines and Technical Basis to address this concern.

EEI, NIPSCO, Southern Companies, and CenterPoint requested clarification in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how and when to manage vulnerability and malicious code reviews of their vendors or contractors and when additional mitigation actions are necessitated. Thank you for the comment. The SDT had previously addressed this concept in the Guidelines and Technical Basis. However, additional changes have been made to clarify further.

Luminant suggested the SDT revise the Guidelines and Technical Basis discussion of Section 1.5 to read, "Disk encryption will not protect a Transient Cyber Asset from unauthorized physical access" and "...Physical Security Perimeter or other physical location that manages physical access...." The SDT thanks you for the comment and has revised the Guidelines and Technical Basis to address this concern. Luminant also recommended deleting the statement "Entities should also consider whether malicious code is a Cyber Security Incident" in the Guidelines. The SDT thanks you for your comment but considers this to be important clarifying language to provide appropriate reminders to entities.

TVA suggested removing the following statement from the Guidelines: "Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004." The SDT appreciates the comment. References to CIP-004 authorizations within the guidance have been updated.

Miscellaneous

Duke Energy, KCPL, and SPP and specific members requested clarification on how often an entity needs to review the Transient Cyber Assets owned or managed by vendors or contractors. Thank you for the comment. The SDT used the concept of a "plan" to allow the entity to define the controls and processes that are most appropriate to

their organization. This includes the timing and frequency of performance of required sections from Attachment 1.

EEI, NIPSCO, and Southern California Edison Company commented that the placement of "CIP Exceptional Circumstances" is unclear in Requirement R4. The SDT agrees with the comment and revised the requirement to address this concern. Thank you for the comment.

EEI, NIPSCO, and Southern Companies commented that some Transient Cyber Assets could fall under both Sections 1 and 2 in certain circumstances and recommended removing "owned" from the requirements. The SDT thanks you for the comment and agrees with the comment. The SDT revised the requirements to address this concern by removing "Owned or" from Sections 1 and 2.

Hydro-Quebec Production commented that the impacts from these requirements are major for utilities. The SDT thanks you for the comment. However, requirement language is needed to address FERC Order No. 791 directives.

IESO and AEP suggested that transient devices requirements should be in the table format and transient devices should be added to the Applicable Systems column. The SDT appreciates the comment. The SDT received strong support for the plan and attachment format to allow entities flexibility in determining how to fulfill the security objectives based on the entity's specific facts and circumstances. Therefore, the SDT determined not to put the requirements into a table format.

MMWEC commented that the requirements should be limited to objectives and not specify controls, which should go in the measures. Thank you for your comment. The SDT discussed your recommendation extensively and chose to keep the bullets in Attachment 1. The SDT considers the options listed in Attachment 1 to be necessary and enforceable requirement obligations supporting Requirement R4.

TVA commented that Requirement R4 and its attachment do not clarify what is included in a plan. The SDT thanks you for your comment. The "Background" section of the Standard includes definitions of what constitutes a plan, program, or process. The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter. Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

TRE suggested the SDT apply the transient devices requirements to low impact. Thank you for your comment. Due to the wide-area impact of the high and medium impact assets, the SDT limited the requirements to those systems. This includes protection when connecting Transient Cyber Assets to multiple-impact rated systems.

EEI, NIPSCO, Southern Companies, Dominion, MRO NERC Standards Review Forum, NV Energy, MidAmerican, and PacifiCorp commented that the use of "Authorized" in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary in that the language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization for the Transient Cyber Asset. The plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address these authorization

elements. Thank you for your comment. In response, the SDT agrees with the comment and revised Attachment 1 to address this concern by changing “specify” to “authorize.”

Southern California Edison suggested that Attachment 1 be revised to clarify the levels of review required based on the control exercised by a Responsible Entity over a Transient Cyber Asset. The language should be revised to describe the requirements when an entity has "full" or "substantial" control through its ownership and management of the asset, as compared when an entity has "minimal" control, as seen when leasing an asset from a vendor. Thank you for your comment. In response, the SDT used the concept of “parties other than the Responsible Entity” to allow the entity to define the controls and processes that are most appropriate to their organization.

AEP commented that the term “security vulnerabilities” is broader than security patch management or malicious code prevention used in CIP-007 and suggested the term be revised. The SDT thanks you for your comment. In response, the SDT revised the term to be “software vulnerabilities.”

Question 4: Transient Devices Definitions

4. *The SDT revised the proposed new definitions for Transient Cyber Assets and Removable Media to address issues raised in stakeholder comments. Do you agree with the proposed definitions? If not, please offer suggested revisions.*

General

CSU agrees with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. Since "Media" is itself not a defined term, CSU recommends either defining "Media" or not capitalizing the term. In response, the SDT replaced "Media" at the beginning of the definition with "Storage media" in order to clarify the term and show it is not a defined NERC Glossary term.

Removable Media

IESO commented that the definition of Removable Media refers to media that are "capable of transmitting executable code to:" and suggested that the word "transmitting" is incorrect and should read "transferring". Media such as floppy disks do not transmit but one can transfer executable code from the disk to another media. In response, the SDT agrees and has modified the language.

Transient Cyber Assets

NPCC commented that based on the new definitions, it is unclear on whether a Cyber Asset can be classified as multiple asset types and would therefore be subject to multiple levels of requirements, i.e. a BES Cyber Asset or a Protected Cyber Asset can also be a Transient Cyber Asset. If a BES Cyber Asset or a PCA also meets the definition of Transient Cyber Asset, there is nothing in the language that says one classification supersedes or precludes another. Solely based on the definitions, it would appear that an entity would have to classify an asset by all the definitions that apply. NPCC recommended:

- Add the following sentence to definition of Transient Cyber Asset: "A Cyber Asset that meets the definition of BES Cyber Asset shall not be considered a Transient Cyber Asset."
- Add a minimum requirement to the PCA definition. "If a PCA is connected for less than 30 days then it is a TCA and more than 30 days it is a PCA."

In response, the intent of the SDT was for an asset to be classified under one definition and therefore subject to only one set of requirements. The SDT revised the definitions to clarify Removable Media is not a Cyber Asset and Transient Cyber Assets are not Protected Cyber Assets.

EEI, Pepco, and Iberdrola commented that for the Transient Cyber Asset definition, the "and" in the parenthesis after "A Cyber Asset," is confusing. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. Also, the parenthetical for the examples is misplaced; it refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and, therefore, unclear as to which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, "directly connected" may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Therefore, EEI recommended changing the definition for Transient Cyber Asset to: "A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." Also, if the intent is for the Transient Cyber Asset

definition to apply to both routable and non-routable communications, EEI requested clarification in the Guidelines and Technical Basis for CIP-010-2. In response, the SDT has made several modifications to the definition of Transient Cyber Asset, as suggested, to address these issues. The SDT has not indicated the directly connection is routable or non-routable, but rather the examples in the definition list several types of direct connections, both routable and non-routable.

FirstEnergy, MMWEC, and Encari did not agree that the CIP Standards adequately specify the scope of devices that can be classified as Transient Cyber Assets. The definitions and standard language make it unclear whether a Transient Cyber Asset needs to be treated as a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity makes a temporary routable connection between a Transient Cyber Asset and an ESP, would this Transient Cyber Asset also have to meet the requirements for the BES Cyber System or for a connected PCA? In other words, could the BES Cyber System requirements also be construed to apply to a Transient Cyber Asset that is temporarily connected? In response, the SDT has modified the definition of Transient Cyber Asset to indicate it is neither a BES Cyber Asset nor a Protected Cyber Asset.

Tri-State G&T noted that the recent revisions made to the Removable Media and Transient Cyber Asset definitions introduced some unintended ambiguity. Revisions should be made to make it clear what the assets/devices must be connected to, in order to clarify this qualifier of the definition. It is our understanding that the intent of the drafting team was to state "...directly connected... [clause]... to..." where the items after the "to" is what the "Cyber Asset" or "Media" is connected to. One simple solution is to add a comma after the [clause] and before the word "to". Another option is to state the [clause] part after the list of what the "Cyber Asset" or "Media" is connected to. In response, the SDT has made revisions to the definition to address this potential ambiguity. The modifier comes before the indicated preposition.

SMUD, FMPA, and BPA agreed with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. However, SMUD is concerned with starting the definition of Removable Media with the capitalized "Media" considering that "Media" is itself not a defined term. In response, the SDT has modified the definition to address these comments.

AEP commented that regarding Transient Cyber Assets, the 30 day timeframe prevents a Responsible Entity from being able to consider a device that is temporarily connected to the BES Cyber System as part of the BES Cyber System, and it is arbitrarily beyond what was ordered by FERC. AEP suggests removing the 30 day timeframe to reduce the amount of tracking Responsible Entities must do with respect to these devices. In response, the entity may designate the device as a PCA and follow the applicable requirements for a PCA. The TCA definition was revised to clarify that a PCA would not be a TCA.

Question 5: Implementation Plan

5. *In response to stakeholder comments, the SDT revised the implementation deadlines. The implementation plan now includes tiered deadlines for the aspects of CIP-003-6. The CIP-007-6 timeframe is now consistent with CIP-006-6. Are these timeframes reasonable and appropriate? If not please explain specifically which implementation plan item needs adjusting and include the rationale for the suggested change.*

Complexity

AEP suggested streamlining the implementation date to the latest date proposed in the Version X and Version 6 implementation plans. KCP&L and SPP & specific members commented that there should be one date for high and medium impact BES Cyber Assets and their accompanying devices and one for low impact BES Cyber Systems. KCP&L and SPP and specific members further recommended that the latest date for each grouping be chosen as a new effective date for all requirements. In response, the SDT thanks you for your comment. With support of stakeholder input, the SDT decided that the added time given under the staggered implementation plan was important to the more labor intensive requirements. While the SDT was unable to move to a later deadline for all requirement areas, in CIP-003, the SDT revised deadline for both sections 2 and 3 to September 1, 2018.

Xcel stated it did not support the revised language providing for tiered deadlines for low impact assets. In response, the SDT thanks you for your comments but states that the majority of industry supports this approach.

Tri-State G&T comments that the timelines are fine, but written in a very convoluted way. It would be helpful to state them more succinctly. In response, NERC will consider creating an informational worksheet to more simply and succinctly see the implementation compliance deadlines.

Protecting LEAP's Before They're Identified

Consumers, EEI, Oncor, Southern Company, MidAmerican, NIPSCO, Duke, First Energy, NV Energy, NRECA, and Hydro Quebec commented on the different effective dates for Elements 2 and 3. Thank you for your comments. In response, the SDT revised the implementation plan to include a September 1, 2018 compliance deadline for CIP-003, Sections 2 and 3.

Excessive Time Period

Texas RE suggests that the proposed implementation time periods are excessive by 12 months, particularly for administrative documentation. Thank you for your comment. The majority of stakeholders supported the proposed deadlines.

Needing More Time

Idaho Power commented that the time frames still do not provide enough time for entities to adjust to an increase in scope of this magnitude. The SDT thanks you for your comment. While the SDT was unable to move to a later deadline for all requirement areas, in CIP-003, the SDT revised the compliance deadline for Section 2 Physical security controls to September 1, 2018.

BPA disagrees with the tiered implementation timeline as currently proposed. BPA believes more time is required to create practices and procedures to implement the policy effectively. BPA suggests that policy (CIP-003-6, R1, part 1.2) be implemented prior to other requirements (CIP-003-6, R2 and CIP-003-6, R2 Attachment 1, items 1-

4). The SDT thanks you for your comment. The SDT was unable to move to a later deadline for all requirement areas, in CIP-003, the SDT revised the compliance deadline for Section 2 Physical security to September 1, 2018.

ACES Standards Collaborators commented that the SDT should consider modifying the implementation dates for electronic access and physical security to be 18 months from the effective date of April 1, 2017. Physical security implementations, depending on the site(s), could have long durations and require additional budget cycles to implement across a diverse geographic and multiple asset types. The SDT thanks you for your comment. The SDT revised the compliance deadline for Section 2 Physical security controls to match the Section 3 Electronic access controls compliance deadline of September 1, 2018, which is 18 months after the April 1, 2017 effective date as ACES proposed.

Support for the Implementation Plan

ATC appreciated the SDT's consideration of previous comments, and supports the adjustments in the implementation plan that accommodate for the time necessary to be successful in implementing Sections 2 and 3 for Low Impact pursuant to CIP-003-6. The SDT thanks you for your support.

SMUD, CSU, Exelon, FMPA, MISO, Occidental Chemical Corporation, NYPA, TVA, NPCC, Dominion, MRO NERC Standards Review Forum, Iberdrola USA, PJM Interconnection LLC, PacifiCorp, Arizona Public Service Company, Encari, Luminant Generation Company, LLC, Rutherford EMC, ATCO Electric, CenterPoint Energy Houston Electric LLC, Manitoba Hydro, Independent Electricity System Operator, Entergy Services, Southern California Edison Company, Pepco Holdings, NRG Energy, and Massachusetts Municipal Wholesale Electric Company supported the implementation plan. The SDT thanks you for your support.

Question 6: Removal of the IAC Language

6. *The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.*

   In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

   Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

The SDT's responses to comments on those revisions are available here.

Question 7: Other Areas Within SAR

7. *Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.*

Some comments from this question were addressed in the previous consideration of comments from the standard drafting team. Those responses only pertained to the revisions in the Version X posting and are available here.

In addition, the SDT addressed the majority of comments in response to this question in other questions in this consideration of comments.

Responses to those not previously addressed are as follows:

Striving for Steady-State

ACES commented on the importance of approving CIP 5 revisions without further changes (so that they are steady-state) to allow for the impacted entities to plan, budget and implement CIP Version 5. The SDT thanks you for your comments and shares the desire to reach a "steady-state" with the CIP standards. The SDT worked to address all four directive issue areas concurrently to respond to the FERC directives in a timely manner. The proposed revisions received passing ballots for all the issue areas in the second posting. However, the SDT felt it important to continue work in response to the constructive comments received and consider further improvements to the revisions. The SDT will post for an additional comment and ballot period and hopes to see additional support for the proposals based on the additional refinements.

NPPD commented that these standards must get to a steady state and changes to the standards should be limited to an absolute minimum. Thank you for your comment. The SDT shares the desire to reach a "steady-state" with the CIP standards. The SDT has worked diligently to address the FERC directives in a timely manner through the NERC iterative, stakeholder process.

Take the Time Needed

AEP urged the SDT to take the time necessary to ensure that the requirements achieve the necessary reliability benefit and that there is broad-based industry support. The SDT thanks you for your comment. The SDT shares AEPs desire to have broad-based industry support for the revisions in response to FERC Order 791. While the revisions for all four issue areas passed stakeholder ballot in the second posting, the SDT felt it important to continue work in response to the constructive comments received. The SDT hopes to see additional support for the proposals based on the additional refinements.

Define Cyber Security Plan

BC Hydro recommended that the term “cyber security plan” be defined or further explained in guidance. Thank you for your comment. The documents developed and implemented in response to CIP-003 R2 are to include the CIP-003 Attachment 1 sections and identify what will essentially become the entity's cyber security plan. The SDT deliberately avoided creating a "Cyber Security Plan" definition, in order to provide entities the flexibility to include these Sections within a more inclusive set of documents, if so desired. For instance, an entity may have an overarching security plan that includes overall physical security, as well as physical security and cyber security for high impact BES Cyber Systems, medium impact BES Cyber Systems, and low impact BES Cyber Systems.

Overly Prescriptive

AEP commented that it was concerned about prescriptive approaches within the standards and the potential to unreasonably restrict the Responsible Entities from defining their own programs. The SDT appreciates the comment. CIP-003-6 Requirement R2 and Attachment 1 have been further revised to strike a balance in FERC's Order 791 determination for greater specificity, providing industry clear options for achieving compliance, as well as flexibility in achieving the Requirement R2 objectives, stated within each Attachment 1 Section. CIP-010-2 R4 and its corresponding Attachment 1 Sections have been further revised as well, seeking the same balance. Many within this SDT and industry believe the current level of specificity, while some may see it as prescriptive, also serves to provide greater predictability and limitations on how various regional auditors might interpret language within those stated objectives.

RSAWs

FMPA commented that their negative votes were due to the current condition of the RSAWs and the status of RAI implementation, in particular on how RAI will address zero tolerance. This SDT submitted comments on the draft RSAWs posted for comment. The SDT continues to be available to work with NERC on RSAWs. In addition, the SDT has forwarded and continues to share the comments on RAI/compliance and enforcement with the relevant NERC divisions. Thank you for your comment.

SMUD also commented that the RSAWs have not sufficiently incorporated the specific language of the standards or the measures. It is unclear from reading the currently posted RSAWs how auditors will use the measures to inform the Compliance Assessment Approach. The SDT submitted comments on the proposed RSAWs during the comment period and continues to be available to work with NERC on RSAWs.

Quality Review

NPC and NYPA recommended quality assurance review before future postings, to avoid reviewers' confusion or need to decipher how to connect related information. Thank you for your comment. The SDT and other resources are in place to conduct a quality review prior to the next posting.

Scope of Nonprogrammable Components

BPA disagreed with the CIP-007-6 R1.2 expansion of scope to non-programmable communication components and proposes re-alignment to R1.1. Thank you for your comment. The SDT confirms that this expands the scope of 1.2, but it does so appropriately and in response to the Order 791 directive to address the security of nonprogrammable components associated with BES Cyber Systems. CIP-007-6 Requirement Part 1.2 concerns the physical security of computing equipment ports. Nonprogrammable components did not previously meet the definition and applicability for Cyber Assets but they may have the same vulnerability that this Requirement Part addresses. The expanded scope closes this gap in protection.

Device Types

MRO suggested that the SDT insert "type" in reference to devices into CIP-010-2 Guidelines and Technical Basis Section 1.1. The SDT thanks you for your comment. While "device types" is one method of grouping TCA devices that entities will likely apply per Attachment 1 Section 1.1, the SDT is reluctant to include this citation within guidance and thereby risk limiting the scope of entity's options for grouping.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02
CIP Version 5 Revisions

Consideration of Comments
Additional Comment Period

October 28, 2014

RELIABILITY | ACCOUNTABILITY




Table of Contents

Consideration of Comments: Project 2014-02 CIP Version 5 Revisions

The Project 2014-02 Drafting Team thanks all commenters who submitted comments on the Critical Infrastructure Protection Version 5 standards. The standards were posted for a 45-day public comment period from September 3, 2014 through October 17, 2014. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 70 responses, including comments from approximately 164 different people from approximately 117 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

This consideration of comments is responding to the comments received on the standards and implementation plan balloted as Version X, which was posted for a 45-day comment period and ballot. There was a concurrent 45-day comment period and ballot for CIP-003-6 and CIP-010-2, which included revisions to address the low impact and transient device directives. The response to the comments received regarding those revisions will be posted when the revisions are posted for an additional comment period and ballot.

All comments submitted may be reviewed in their original format on the standards' project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards, Valerie Agnew, at 404-446-2566 or at valerie.agnew@nerc.net . In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Introduction

The SDT appreciates industry comments on the revisions to the CIP Reliability Standards. During the development of the revised standards prior to posting, the SDT made it a priority to conduct outreach as modifications were made to the standards. The SDT conducted one face-to-face meeting to revise the standards, Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs) in order to appropriately consider all comments received. The SDT continues its rigorous conference call schedule as it understands the importance of getting these standards to steady state.

Background

On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards and also directed that NERC make the following modifications to those standards:

1. Modify or remove the "identify, assess, and correct" (IAC) language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for to assets containing low impact BES Cyber Systems.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the IAC language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the low impact and transient electronic devices directives. The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.

Question 6: Version X

6. *The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.*

   In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

   Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

Many commenters expressed support for the removal of the IAC language through a 'yes' response to Question 6 without any additional comments. Those commenters include American Transmission Company LLC, FirstEnergy, Tennessee Valley Authority, Northeast Power Coordinating Council, Dominion, MRO NERC Standards Review Forum, Duke Energy, Iberdrola USA, PJM Interconnection LLC, Edison Electric Institute, Oncor, Arizona Public Service Company, Encari, Luminant Generation Company, LLC, ATCO Electric, Idaho Power, Manitoba Hydro, Independent Electricity System Operator, Texas Reliability Entity, Entergy Services, Inc., Southern California Edison Company, Pepco Holdings Inc., Hydro-Quebec Production, Kansas City Power & Light, Consumers Energy Company, NV Energy, Massachusetts Municipal Wholesale Electric Company, and Tri-State Generation and Transmission Association, Inc.

Support IAC Removal but Comments on Zero Tolerance and Lows

Florida Municipal Power Agency (FMPA), BC Hydro, Indiana Municipal Power Agency (IMPA), and ACES Standards collaborators supported the removal of the IAC language but expressed concern over zero tolerance requirements. While the removal of the IAC language returns the requirements to a zero tolerance construct, NERC is implementing risk-based compliance monitoring and enforcement processes to address the zero tolerance concerns. The SDT will forward concerns raised with compliance and enforcement to the relevant NERC departments. In response to IMPA, NERC is making an informational filing with FERC regarding the risk-based Compliance Monitoring and Enforcement Program on or about October 31, 2014. In response to ACES Standards collaborators, the risk-based compliance monitoring and enforcement processes will all be implemented by January 1, 2015.

Calpine agrees with removing IAC from the standards for high and medium impact categories but recommended keeping IAC for the low impact category. In response, Calpine did not further explain its rationale for its recommendation, but the SDT determined that using the IAC language for different classification levels would not appropriately address the FERC directive.

FMPA requested additional clarity in the Reliability Standard Audit Worksheets (RSAWs) as the currently posted RSAWs do not provide enough clarity and guidance on compliance expectations to understand if zero tolerance concerns have been addressed. NERC is reviewing the comments made to the RSAWs. In response, while the removal of the IAC language returns the requirements to a zero tolerance construct, NERC is implementing risk-based compliance monitoring and enforcement processes to address the zero tolerance concerns. The SDT will forward concerns raised with compliance and enforcement to the relevant NERC departments.

Expectations for RAI and its Fulfillment of the IAC Intent

SPP and specific members commented that the RAI program is not complete and has not been used in the audit and enforcement process, and it requires a significant amount of trust. In response, while the removal of the IAC language returns the requirements to a zero tolerance construct, NERC is implementing risk-based compliance monitoring and enforcement processes to address the zero tolerance concerns. Risk-based compliance monitoring and enforcement processes are already in use.

CenterPoint Energy Houston Electric LLC supported this revision approach for IAC. As proposed by NERC, the Company looks forward to the concepts of IAC being implemented within the final framework of the RAI. MISO, Occidental Chemical Corporation, Sacramento Municipal Utility District (SMUD), MidAmerican Energy Company, American Electric Power, and Xcel Energy supported the removal of IAC in the timeframe ordered by FERC and supported the continued work by NERC to develop RAI. In contrast, Rutherford EMC commented that the IAC language provided a more proactive results-based approach to truly identify, assess, and correct problems rather than follow standards. In response to all commenters, for additional information regarding how the concepts of IAC will be implemented within the risk-based compliance monitoring and enforcement framework, please see *The Application of Risk-based Compliance Monitoring and Enforcement Program Concepts to CIP Version 5*[2], available on NERC's RAI web page.

Does Not Support Removal

Nebraska Public Power District (NPPD) and City of Austin d/b/a Austin Energy commented that they do not support the removal of the IAC language. NPPD and Austin Energy went on to suggest that either the requirements containing IAC be removed entirely or to keep the IAC language as is in Version 5. As stated in the prior consideration of comments, the SDT states that FERC approved the security control requirements within Version 5, but found the IAC language related to compliance to the requirements and objected to its inclusion in the requirement itself. The SDT will forward concerns raised with compliance and enforcement to the relevant NERC departments.

Completing Revisions to all Four Directive Areas

Exelon Companies commented that it strongly supports the SDT's efforts to complete revisions in all four directive areas by the February 3, 2015 filing deadline. Similarly, National Rural Electric Cooperative Association (NRECA) supported the Version X package and is hopeful the SDT can successfully complete revisions to CIP Version 5 for the four directive areas by the February 3, 2015 filing deadline. NRECA went on to state that by having the four directive areas addressed by the filing deadline will be critical to achieve a steady-state of NERC CIP standards. In response, the SDT continues its work with the intent of completing revisions responding to all four FERC directive areas.

[2] http://www.nerc.com/pa/CI/tpv5impmntnstdy/Public_Final_Application_Risk-Based_CMEP_Concepts_to_CIPV5_(10-22-2014).pdf

Question 7: Other Areas Within SAR

7. *Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.*

Some comments from this question will be addressed in a future consideration of comments from the standard drafting team. The responses below only pertain to the revisions in the Version X posting.

Communication Networks

Bonneville Power Administration (BPA) commented that CIP-007-6, Requirement R1, Part 1.2 expands the scope of the requirement to nonprogrammable communication components and suggested that Part 1.2 be revised to align with Part 1.1. In addition, BPA requested additional guidance on the specific nonprogrammable communication components located inside both a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP). The SDT confirms this expands the scope of Part 1.2, but it does so appropriately and in response to the Order No. 791 directive to address the security of nonprogrammable components associated with BES Cyber Systems. CIP-007-6, Requirement R1, Part 1.2 concerns the physical security of computing equipment ports. Nonprogrammable components did not previously meet the definition and applicability for Cyber Assets but they may have the same vulnerability this Requirement Part addresses. The expanded scope closes this gap in protection. In response to the request for additional guidance, the SDT added a diagram to the Guidelines and Technical Basis section of CIP-007-6 to further illustrate the intent behind including components inside both a PSP and an ESP.

FMPA and EEI requested clarification on whether an entity can violate CIP-007-6, Requirement R2, Part 2.3 while still meeting Part 2.4. The SDT appreciates the comment but notes that the SDT did not focus on this requirement during its revisions. However, the SDT notes that CIP-007-5, R2, Requirement 2, Part 2.4 allows an entity to modify an existing mitigation plan that is created in Part 2.3. The Requirement Part language allows for "an extension to the timeframe specified in Part 2.3" and have the extension "approved by the CIP Senior Manager or delegate."

Version X

NRG Energy suggested removing the word “shall” from all the sections in the attachment. The SDT appreciates the comment but notes that the attachments were not included as part of the Version X package. The SDT will respond to this comment along with other comments related to the low impact and transient devices revisions.

General

City of Austin d/b/a Austin Energy commented that the CIP Version 5 standards have been difficult to implement, and it would like the standards to get to steady-state with minimal revisions. The SDT appreciates the comment and notes that its focus was on the four directive areas for these revisions. Furthermore, the SDT continues its work with the intent of completing revisions to get to steady-state.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

See Implementation Plan for CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save

the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the standard. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements of the standard.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the requirements of the standard. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements of the standard.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5.1, Requirement R1, Part R1.3, shall implement one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the

specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 18 calendar months of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 15 calendar months but did complete this review	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 16 calendar months but did	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2)	The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R4)	calendar days but did document this change in less than 50 calendar days of the change. (R4)	calendar days of the change. (R4)	from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate for its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-6, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.**~~

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. ~~3.~~ Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for ~~an additional comment and ballot to ballot the removal of "identify, assess, and correct" language~~final ballot. The draft includes modifications to meet the FERC Order No. 791 directive~~s to remove or modify the "identify, assess, and correct" language from CIP-003~~.

Anticipated Actions	Anticipated Date
~~Additional 45-Day Comment Period~~	~~September 2014~~
Final Ballot is Conducted	October~~/November~~ 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
~~X~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~X~~6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~X~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

~~Reliability Standard CIP-003-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.~~

~~Registered Entities shall not be required to comply with Reliability Standard CIP-003-X, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-X~~See Implementation Plan for CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards

could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System~~BES. A review of UFLS tolerances defined within ~~regional~~ Regional ~~reliability~~ Reliability ~~standards~~ Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the ~~standard's~~ requirements of the standard. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the ~~standard's~~ requirements of the standard.

Annual review and approval of the cyber security policy ensures that the policy is kept~~-~~ up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the ~~standard's~~ requirements of the standard. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the ~~standard's~~ requirements of the standard.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5.1, Requirement R1, Part R1.3, shall implement one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP ~~senior~~ Senior ~~manager~~ Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These

delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 18 calendar months of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 15 calendar months but did complete this review	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 16 calendar months but did	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2)	The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6~~X~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6~~X~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R4)	calendar days but did document this change in less than 50 calendar days of the change. (R4)	calendar days of the change. (R4)	from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-~~X~~6, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~X~~6, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-~~X~~6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate ~~to~~ for its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-~~X~~6, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~X~~6, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems

is not necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-~~X~~6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that ~~this~~ the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~X~~6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity ~~should have~~ significant flexibility to adapt this requirement to ~~their~~ its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records ~~provides~~ shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations ~~up~~ up ~~to~~ to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment ~~(March 20, 2008).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014
~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

~~Effective Dates~~

1. ~~**24 Months Minimum –** CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.~~

2. ~~In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated ~~version number~~Version Number from -2 to -3 ~~Approved by~~ In Requirement 1.6, deleted the ~~NERC Board of Trustees.~~ sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	~~Update to conform to changes to CIP-002-4 (Project 2008-06)~~
5	~~TBD~~11/26/12	Adopted by the NERC Board of Trustees.~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-003-5.	

~~Definitions of Terms Used in the Standard~~

~~*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*~~

When this standard has received ballot approval, the text boxes will be moved to the ~~"~~Application Guidelines ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~5~~6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

See Implementation Plan for CIP-003-6.

6. Background:

Standard CIP-003~~-5~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the ~~Bulk Electric System.~~BES. A review of UFLS tolerances defined within ~~regional reliability standards~~Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

~~**Rationale – R1:**~~

~~One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.~~

~~Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the standard. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements of the standard.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);

1.7 Configuration change management and vulnerability assessments (CIP-010);

1.8 Information protection (CIP-011); and

1.9 Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

~~**Rationale – R2:**~~

~~One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.~~

~~The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.~~

~~Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

Rationale for Requirement R2:

One or more security policies enable effective implementation of the requirements of the standard. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements of the standard.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5.1, Requirement R1, Part R1.3, shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

~~**Rationale – R3:**~~

~~The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business

models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

~~**Rationale – R4:**~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve asAs defined in the NERC Rules of Procedure, "Compliance Enforcement Authority (" (CEA") unless) means NERC or the applicable entity is owned, operated, or controlled byRegional Entity in their respective roles of monitoring and enforcing compliance with the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEANERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance AuditAudits

Self-CertificationCertifications

Spot Checking

Compliance InvestigationViolation Investigations

Self-Reporting

- Complaint

Complaints

1.4. **Additional Compliance Information:**

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		within 18 calendar months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only three~~one of the topics as required by Requirement R2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (R2) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only~~ two of the topics as required by Requirement R2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (R2) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only one~~three of the topics as required by Requirement R2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (R2) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the~~	The Responsible Entity did not ~~document or implement~~have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	~~security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar	~~topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by	Requirement R2 within 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	Requirement R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40	~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or~~	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R4)	calendar days but did document this change in less than 50 calendar days of the change. (R4)	~~correct the deficiencies.(R4)~~ ~~OR~~ ~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4)~~ ~~OR~~ The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60	from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					calendar days of the change. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-~~5~~6, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~5~~6, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-~~5~~6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate ~~to~~for its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-~~5~~6, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-~~5~~6, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems

is not necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-~~5~~6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that ~~this~~the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-~~5~~6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity ~~should have~~ significant flexibility to adapt this requirement to ~~their~~its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records ~~provides~~shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up~~-~~to~~-~~date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for final ballot. The draft includes modifications to meet FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-6.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to

provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or			incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR The Responsible Entity has implemented	individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last

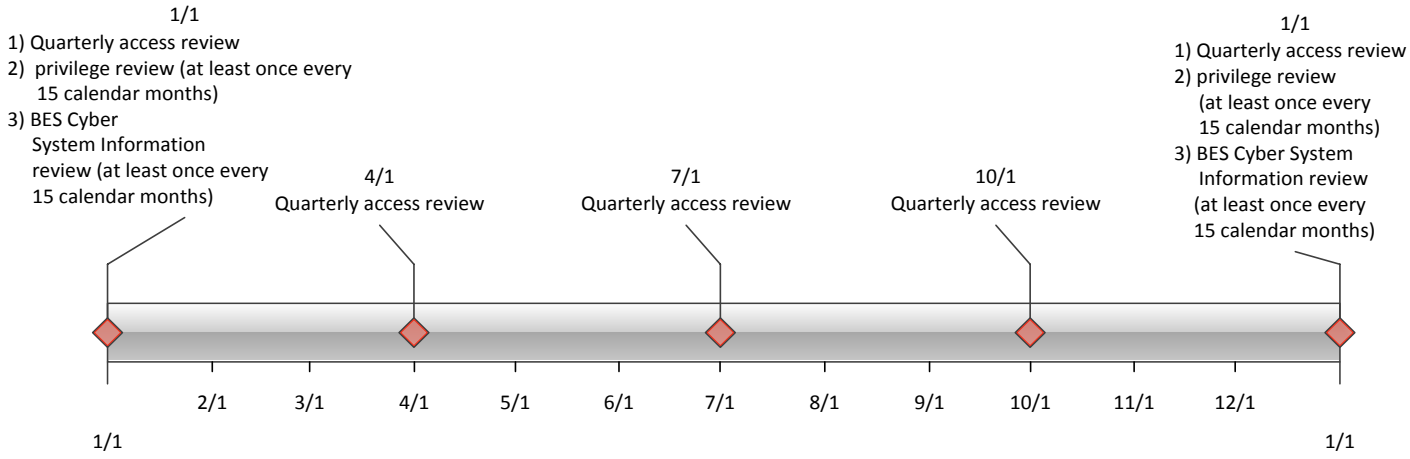
PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the

individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.**~~

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. ~~3.~~ Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for ~~an additional comment and ballot to ballot the removal of "identify, assess, and correct" language~~final ballot. The draft includes modifications to meet FERC Order No. 791 directive~~s to remove or modify the "identify, assess, and correct" language from CIP-004~~.

Anticipated Actions	Anticipated Date
~~Additional 45-Day Comment Period~~	~~September 2014~~
Final Ballot is Conducted	October~~/November~~ 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
~~X~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~X~~6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~X~~6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~Reliability Standard CIP-004-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction~~See Implementation Plan for CIP-004-6.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the ~~requirement's~~ common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~X~~ 6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for

CIP-004-~~X~~ 6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~X~~ 6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~X~~ 6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~X~~ 6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~X~~ 6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~X~~ 6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~X~~ 6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-~~X~~6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-~~X~~6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~X~~ 6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~X~~ 6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~X~~ 6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-~~X~~ 6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ 6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~X~~ 6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~X~~ 6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~X~~ 6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-~~X~~ 6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~X~~ 6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity	did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			(3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or			unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR The Responsible Entity has implemented	individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last

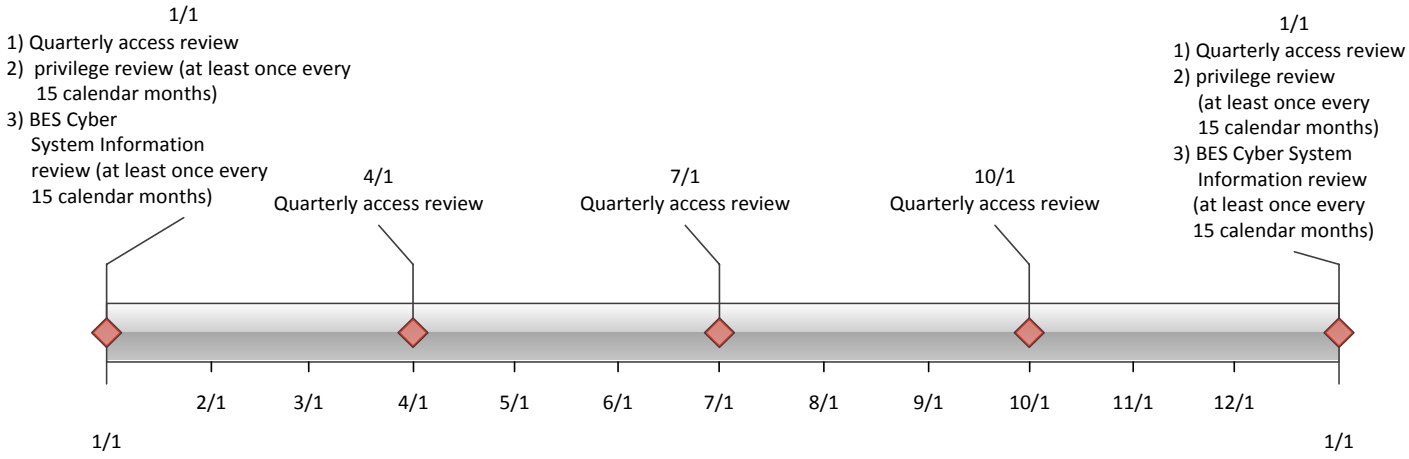
PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the

individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment ~~(March 20, 2008).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014

3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives

4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted for final ballot. The draft includes modifications to meet FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014
~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

Effective Dates

1. **24 Months Minimum –** CIP-004-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	~~12/30/10~~1/24/11	~~Modified to add specific criteria for Critical Asset identification.~~ Approved by the NERC Board of Trustees.	~~Update~~
~~4~~5	~~1/24/~~11/26/12	~~Approved~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata

~~Definitions of Terms Used in the Standard~~

~~*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*~~

When this standard has received ballot approval, the text boxes will be moved to the ~~"~~Application Guidelines ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~5.1~~6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~5.1~~6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-6.

6. Background:

Standard CIP-004 ~~5.1~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~]~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the ~~requirement's~~ common subject matter of the requirements.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table~~. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities~~.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a

response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes

Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

~~**Rationale for R1:** Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.~~

~~**Summary of Changes:** Reformatted into table structure.~~

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
		authorized unescorted physical access to BES Cyber Systems.	information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

~~Reference to prior version:~~ ~~*CIP-004-4, R1*~~	**~~Change~~ Rationale~~: *Changed to remove*~~ for Requirement R2:** To ensure that the Responsible Entity's training program for personnel who need ~~*to ensure or prove everyone with*~~ authorized electronic access and/or authorized unescorted physical access ~~*"received" ongoing reinforcement – to state that security awareness has been reinforced.*~~ ~~*Moved example mechanisms to guidance.*~~to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

~~Rationale for R2:~~ ~~To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.~~

~~Based on their role, some personnel may not require training on all topics.~~

~~Summary of Changes:~~

~~1. Addition of specific role training for:~~

- ~~The visitor control program~~
- ~~Electronic interconnectivity supporting the operation and control of BES Cyber Systems~~
- ~~Storage media as part of the handling of BES Cyber Systems information~~

~~2. Change references from Critical Cyber Assets to BES Cyber Systems.~~

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies, a~~ one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.1*~~		~~**Change Rationale:** *Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*~~	

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.1*~~		~~**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*~~	
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

~~Reference to prior version:~~	~~Change~~ Rationale~~: *Updated*~~ for Requirement R3:
~~*CIP004-4, R2.3*~~	To ensure that individuals who need authorized electronic or authorized unescorted physical access to ~~*replace "annually"*~~BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with ~~*"once every 15 calendar months."*~~ access must have had a personnel risk assessment completed within the last 7 years.

~~**Rationale for R3:** To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.~~

~~**Summary of Changes:** Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.~~

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment ~~programs~~program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
~~**Reference to prior version:**~~ ~~*CIP004-4, R3.1*~~		~~**Change Rationale:** *Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*~~	

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

~~**Reference to prior version:**~~ ~~*CIP004-4, R3.1*~~CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program	~~**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*~~

~~CIP-004-5.1 Table R3 – Personnel Risk Assessment Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
~~Reference to prior version:~~ ~~*NEW*~~		~~Change Rationale: *There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.*~~	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

~~Reference to prior version:~~ ~~*CIP-004-4, R3.3*~~	~~Change Rationale: *Separated into its own table item.*~~		
CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

~~Reference to prior version:~~

~~*CIP-004-3, R3, R3.3*~~

~~Change~~ Rationale~~: *Whether*~~ **for** ~~*initial access or maintaining access, establishes*~~**Requirement R4:**

To ensure that ~~*those*~~individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must ~~*have had PRA completed within 7 years.*~~address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This ~~*covers both initial and renewal.*~~is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The ~~*implementation plan specifies that initial performance*~~focus of this requirement is ~~*7 years after the last personnel risk assessment*~~on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that ~~*was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.*~~ the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

~~Rationale for R4:~~ ~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.~~

~~Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).~~

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

~~Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.~~

~~If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.~~

~~For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.~~

~~Summary of Changes:~~ ~~The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.~~

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program. [Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Reference to prior version: *CIP-003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1*	**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.CIP-004-5.16 Table R4 – Access Management Program

~~CIP-004-5.1 Table R4 – Access Management Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

~~**Reference to prior version:**~~ ~~*CIP-004-4, R4.1*~~	~~**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*~~CIP-004-~~5~~.16 Table R4 – Access Management Program

~~CIP-004-5.1 Table R4 – Access Management Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

~~*Reference to prior version:*~~ ~~*CIP-007-4, R5.1.3*~~CIP-004-~~5.1~~6 Table R4 – Access Management Program	~~**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.*~~

~~CIP-004-5.1 Table R4 – Access Management Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

~~Reference to prior version:~~ *~~CIP-003-4, R5.1.2~~*	**~~Change Rationale:~~** *~~Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.~~***Rationale for Requirement R5:** The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner. In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination. Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

~~**Rationale for R5:** The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.~~

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.~~

~~Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).~~

~~**Summary of Changes:** FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).~~

~~As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."~~

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation*. *[Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

~~Reference to prior version:~~ **CIP-004-**~~4, R4.2~~6 Table R5 – Access Revocation	**~~Change Rationale:~~** ~~*The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* **to require immediate revocation** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*~~

~~CIP-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

~~Reference to prior version:~~ **CIP-004-~~4, R4.2~~6 Table R5 – Access Revocation**	**~~Change Rationale:~~** *~~FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.~~*

~~CIP-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

Reference to prior version: NEWCIP-004-5.16 Table R5 – Access Revocation	**Change Rationale:** *FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*

~~CIP-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Reference to prior version: NEWCIP-004-5.16 Table R5 – Access Revocation	**Change Rationale:** FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

~~CIP-004-5.1 Table R5 – Access Revocation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.
~~**Reference to prior version:**~~ ~~*CIP-007-4, R5.2.3*~~		~~**Change Rationale:**~~ ~~*To provide clarification of expected actions in managing the passwords.*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~(""~~ (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Violation Investigations

Self-Reporting

- ~~Complaint~~

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	~~and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized	~~and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	~~identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date~~, and did not identify, assess and correct the deficiencies~~. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals~~, and did not identify, assess, and~~	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals~~, and did not identify, assess, and~~	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	~~correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	~~correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date ~~and has identified deficiencies, and did not identify, assess, and correct the deficiencies~~. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)			
R4	**Operations Planning and Same Day Operations**	~~Lower~~Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter~~, and did not identify, assess and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located~~, and did not identify, assess, and correct the deficiencies~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.4)			were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that~~-~~ an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances~~, and did not~~			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~identify, assess, and correct the deficiencies~~. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last

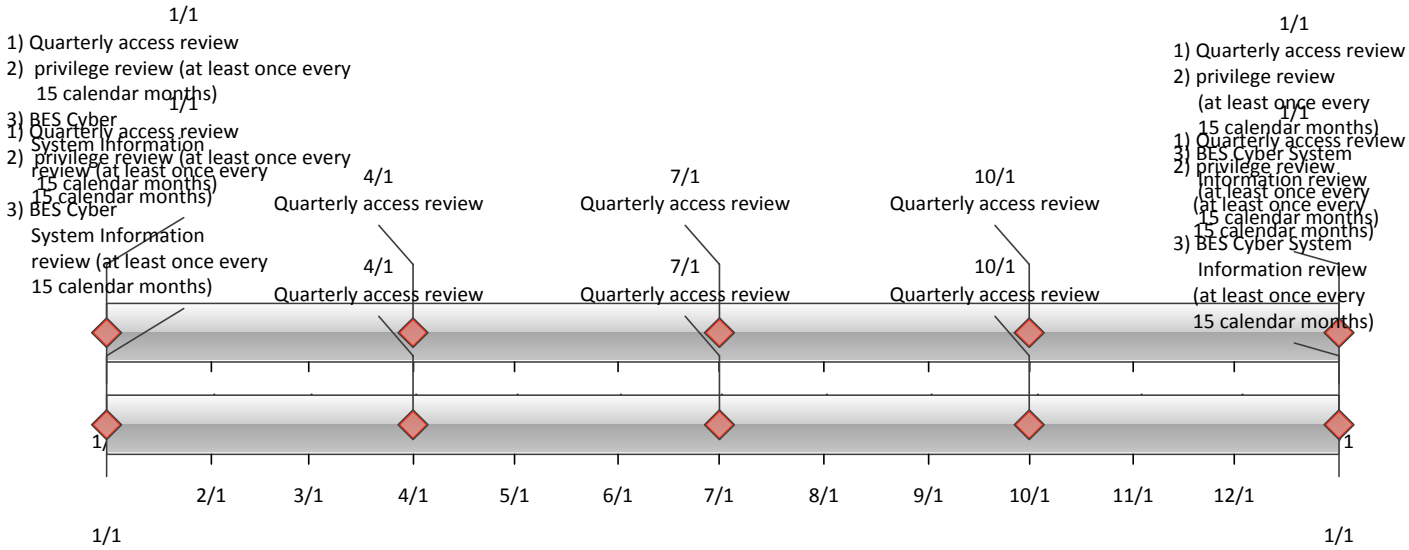
PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to

or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for final ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-006-6.

6. Background:

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented

processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Medium**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for an additional comment period and ballotfinal ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
~~6~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.~~

~~For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6~~See Implementation Plan for CIP-006-6.

6. Background:

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Medium**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus ~~is~~ of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances ~~this~~ a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter~~'s controls~~ could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person ~~they are~~the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-~~3~~ 2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment ~~(March 20, 2008).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted for final ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014

~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014
~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

Effective Dates

1. **24 Months Minimum –** CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	~~TBD~~11/26/12	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	

~~Definitions of Terms Used in the Standard~~

~~*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*~~

When this standard has received ballot approval, the text boxes will be moved to the ~~"~~Application Guidelines ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-~~5~~6

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-006-6.

6. Background:

Standard CIP-006~~-5~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~].~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the~~

~~documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

~~**Rationale:** Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*~~

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

~~**Summary of Changes:** The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.~~

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented physical security ~~plans~~plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~5~~6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~5~~6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~5~~6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.
~~Reference to prior version:~~ *~~CIP-006-4c, R2.1 for Physical Access Control Systems~~* *~~New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity~~*		**~~Change Description and Justification:~~** ***~~Change Description and Justification:~~*** *~~To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.~~*	

CIP-006-~~5~~6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

~~Reference to prior version:~~ ~~*CIP006-4c, R3 & R4*~~ CIP-006-6 Table R1 – Physical Security Plan	~~**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*~~

~~CIP-006-5 Table R1 – Physical Security Plan~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

~~**Reference to prior version:**~~ ~~CIP006-4c, R3 & R4~~	~~**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.*~~ ~~*Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.*~~ ~~*FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*~~ CIP-006-6 Table R1 – Physical Security Plan

~~CIP-006-5 Table R1 – Physical Security Plan~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
~~**Reference to prior version:**~~ ~~*CIP006-4c, R5*~~		~~**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*~~	

~~CIP-006-5 Table R1 – Physical Security Plan~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
~~**Reference to prior version:**~~ ~~*CIP006-4c, R5*~~		~~**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*~~	
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

~~CIP-006-5 Table R1 – Physical Security Plan~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~Reference to prior version:~~ ~~CIP006-4c, R5~~		**~~Change Description and Justification:~~** ~~*Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*~~	
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

~~Reference to prior version:~~ ~~CIP006-4c, R5~~		~~Change Description and Justification: Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems~~ CIP-006-6 Table R1 – Physical Security Plan	
Part	**Applicable Systems**	**Requirements**	**Measures**

~~CIP-006-5 Table R1 – Physical Security Plan~~			
~~**Part**~~	~~**Applicable Systems**~~	~~**Requirements**~~	~~**Measures**~~
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

~~**Reference to prior version: CIP-006-4c, R6**~~	~~*Change Description and Justification: CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.*~~ ~~*Examples of logging methods have been moved to the Guidelines and Technical Basis section.*~~ CIP-006-6 Table R1 – Physical Security Plan

~~CIP-006-5 Table R1 – Physical Security Plan~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~**Reference to prior version:** CIP-006-4c, R7~~1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	~~**Change Description and Justification:** *No change.*~~Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

~~**Rationale:** To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.~~

~~**Summary of Changes:** Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.~~

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented visitor control ~~programs~~program(s) that include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

~~Reference to prior version:~~ **CIP-006-~~4c, R1~~ 6** ~~2~~ Table R2 – Visitor Control Program	**~~Change Description and Justification:~~** ~~*Added the ability to not do this during CIP Exceptional Circumstances.*~~

~~CIP-006-5 Table R2 — Visitor Control Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
~~**Reference to prior version:**~~ ~~*CIP-006-4c R1.6.1*~~		~~**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.*~~	

~~CIP-006-5 Table R2 — Visitor Control Program~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

~~**Reference to prior version:** CIP-006-4c, R7~~	~~**Change Description and Justification:** *No change*~~ **Rationale for Requirement R3:** To ensure all Physical Access Control Systems and devices continue to function properly.

~~**Rationale:** To ensure all Physical Access Control Systems and devices continue to function properly.~~

~~**Summary of Changes:** Reformatted into table structure.~~

~~Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.~~

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing ~~programs~~program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

CIP-006-~~5~~6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
~~**Reference to prior version:**~~ ~~*CIP-006-4c, R8.1 and R8.2*~~		~~**Change Description and Justification:** *Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority~~ ("" (~~CEA"") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

~~• Complaint~~

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A ~~The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8)~~ ~~OR~~	N/A ~~The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to~~	N/A ~~The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5)~~ ~~OR~~	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) ~~OR~~ ~~The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for~~	~~identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)~~	~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not~~	~~The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1)~~ OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)~~		~~assess or correct the deficiencies. (1.6)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)~~	~~but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2)~~ OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4)~~ OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical ~~security~~ Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Same-Day Operations**	**Medium**	N/A	N/A ~~The Responsible Entity included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or~~	N/A ~~The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)~~	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)~~		retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	~~Lower~~**Medium**	The Responsible	The Responsible Entity has documented and	The Responsible Entity has documented and	The Responsible Entity ~~has~~ did not document~~ed~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	~~and~~ or implement~~ed~~ a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus ~~is~~of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances ~~this~~a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, ~~a sole perimeter's~~ controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person ~~they are~~the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.~~7~~6 and 1.~~8~~7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be

implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each SPS or RAS where the SPS or RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-007-6.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-6 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

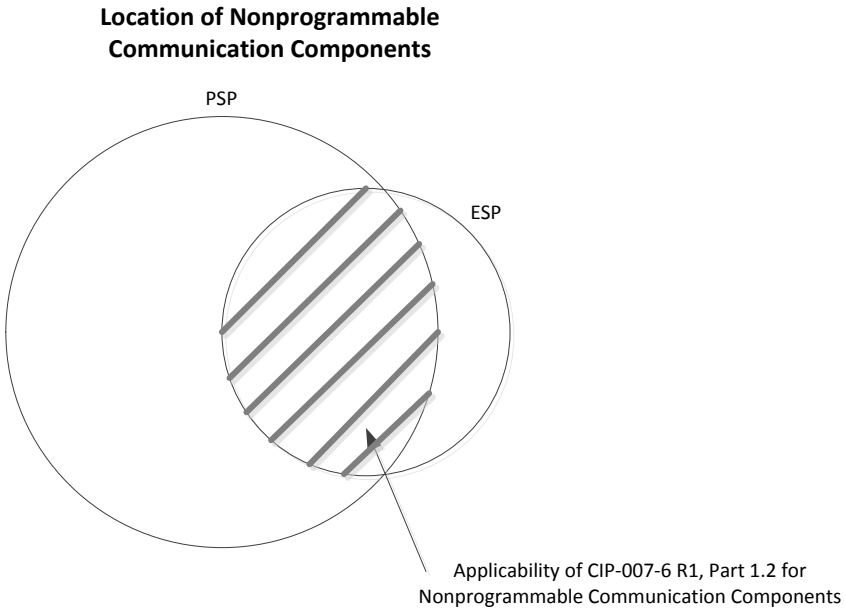
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.**~~

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. ~~3.~~ Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for ~~an additional comment and ballot to ballot the removal of "identify, assess, and correct" language~~final ballot. The draft includes modifications to meet the FERC Order No. 791 directive~~s to remove or modify the "identify, assess, and correct" language from CIP-007~~.

Anticipated Actions	Anticipated Date
~~Additional 45-Day Comment Period~~	~~September 2014~~
Final Ballot is Conducted	October~~/November~~ 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
~~X~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-~~X~~6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~X~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~Reliability Standard CIP-007-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.~~

~~Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-X, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-X~~See Implementation Plan for CIP-007-6.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~X~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~X~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~X~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~X~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~X~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~X~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~X~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~X~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~X~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~X~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~X~~ 6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~X~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~X~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~X~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~X~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~X~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~X~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~X~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or ~~Removable~~ removable ~~Media~~media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~X~~6 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	any processes for installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or	CIP-007-~~X~~6 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3)~~es~~.	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6~~X~~ Table R3. (R3)~~ies~~. OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~X~~6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~X~~6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~X~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

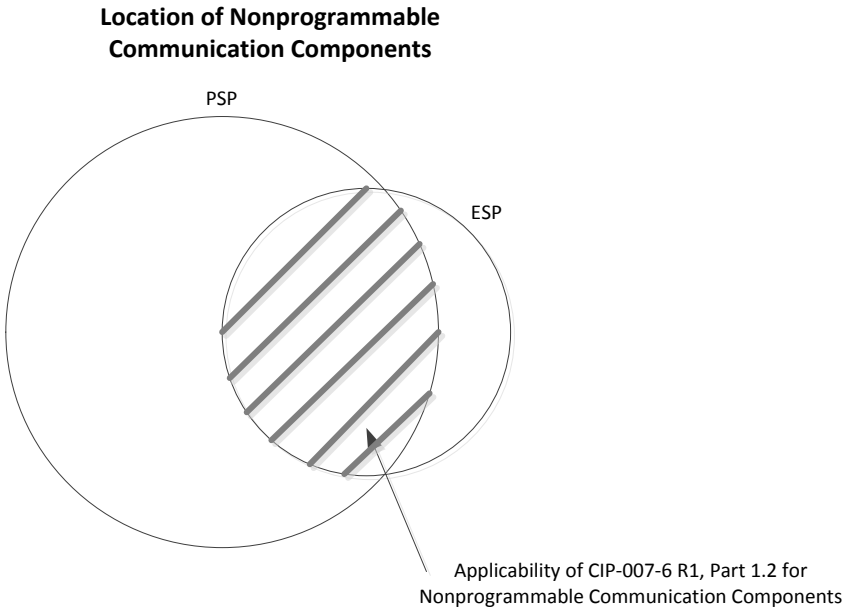
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense ~~are~~ is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~.~~



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. ~~Stand-alone~~Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where

security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related

patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor

the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail ~~etc~~etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment ~~(March 20, 2008).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014

~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

Effective Dates

1. **24 Months Minimum –** CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated ~~version number~~Version Number from -2 to -3 ~~Approved by~~ In Requirement 1.6, deleted the ~~NERC Board of Trustees.~~ sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	~~12/30/10~~1/24/11	~~Modified to add specific criteria for Critical Asset identification.~~ Approved by the NERC Board of Trustees.	~~Update~~
~~4~~5	~~1/24/~~11/26/12	~~Approved~~Adopted by the NERC Board of Trustees.	~~Update~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	~~TBD~~11/22/13	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~FERC Order issued approving CIP-007-5.	

~~Definitions of Terms Used in the Standard~~

~~*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*~~

When this standard has received ballot approval, the text boxes will be moved to the ~~"~~Application Guidelines ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-~~5~~6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System (SPS) or Remedial Action Scheme (RAS) where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS where the ~~Special Protection System~~SPS or ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-007-6.

6. Background:

Standard CIP-007~~-5~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5~~, which requires the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~]~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the~~

~~documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

~~**Rationale for R1:** The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~**Summary of Changes:** Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.~~

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
~~**Reference to prior version:** *CIP-007-4, R2.1 and R2.2*~~		~~**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*~~	

CIP-007-~~5~~6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
~~**Reference to prior version:** *NEW*~~		~~**Change Description and Justification:** *On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*~~	

~~**Rationale for R2:** Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.~~

~~**Summary of Changes:** The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.~~

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.
~~**Reference to prior version:**~~ ~~*CIP-007, R3*~~		~~**Change Rationale:** *The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*~~	

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.
~~**Reference to prior version:**~~ ~~*CIP-007, R3.1*~~		~~**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 35-day time frame.*~~	

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~5~~6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~Reference to prior version:~~ ~~*CIP-007, R3.2*~~		**~~Change Rationale:~~** ~~*The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*~~	
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

~~Reference to prior version:~~ ~~*CIP-007, R3.2*~~	**~~Change~~ Rationale~~:~~ ~~*Similar to*~~ for Requirement R3:** Malicious code prevention has the ~~*current wording but added that*~~purpose of limiting and detecting the ~~*plan must be implemented within*~~addition of malicious code onto the ~~*timeframe specified in*~~applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the ~~*plan,*~~availability or ~~*in a revised plan as approved by*~~integrity of the ~~*CIP Senior Manager or delegate.*~~ BES Cyber System.

~~**Rationale for R3:** Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~**Summary of Changes:** In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.~~

~~Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"~~

~~In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.~~

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
~~**Reference to prior version:**~~ ~~*CIP-007-4, R4; CIP-007-4, R4.1*~~		~~**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*~~	

CIP-007-~~5~~6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
~~**Reference to prior version:**~~ ~~*CIP-007-4, R4*~~ ~~*CIP-007-4, R4.1*~~		~~**Change Rationale:** *See the Summary of Changes.*~~	

CIP-007-~~5~~6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

~~Reference to prior version:~~ ~~*CIP-007-4, R4; CIP-007-4, R4.2*~~	**~~Change~~ Rationale~~:~~ for Requirement** ~~*essentially unchanged from previous versions; updated*~~**R4:** Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to ~~*refer to previous parts of the*~~ support post-event data analysis. Audit processing failures are not penalized in this requirement ~~*table.*~~. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

~~**Rationale for R4:** Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security related logs is intended to support post event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~**Summary of Changes:** Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."~~

~~The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.~~

~~In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.~~

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
~~**Reference to prior version:**~~ ~~*CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, andR6.3*~~		~~**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*~~	

CIP-007-~~5~~6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.
~~**Reference to prior version:**~~ ~~*CIP-005-4, R3.2; CIP-007-4, R6.2*~~		~~**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.*~~	

CIP-007-~~5~~6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
~~**Reference to prior version:** *CIP-005-4, R3.2; CIP-007-4, R6.4*~~		~~**Change Rationale:** *No substantive change.*~~	
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

~~Reference to prior version:~~ *~~CIP-005-4, R3.2; CIP-007-4, R6.5~~*	**~~Change Description and Justification:~~** *~~Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.~~* **Rationale for Requirement R5:** To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised. Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time. Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

	Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement. Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords. For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

~~Rationale for R5:~~ ~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

~~Summary of Changes (From R5):~~

~~CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.~~

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the

same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
~~**Reference to prior version:**~~ ~~*CIP-007-4, R5*~~		~~**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*~~	

CIP-007-~~5~~6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

~~Reference to prior version:~~ ~~CIP-007-4, 6 Table R5.2 and R5.2.3~~ ~~— System Access Control~~	**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*

~~CIP-007-5 Table R5 – System Access Control~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

~~Reference to prior version:~~ **CIP-007-~~4~~6 Table R5~~.2~~.2 – System Access Control**	**~~Change Rationale:~~** *~~No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.~~*

~~CIP-007-5 Table R5 — System Access Control~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

~~Reference to prior version:~~ **CIP-007-~~4~~6 Table R5~~.2.1~~ – System Access Control**	**~~Change Rationale:~~** ~~*The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*~~

~~CIP-007-5 Table R5 – System Access Control~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

~~Reference to prior version:~~ **CIP-007-~~4~~6 Table R5~~2~~** **– System Access Control**	**Change Rationale:** ~~*CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*~~

~~CIP-007-5 Table R5 – System Access Control~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

~~Reference to prior version:~~ **CIP-007-~~4~~6 Table R5~~ 3.3~~ – System Access Control**	**~~Change Rationale:~~** ~~*This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.~~

~~CIP-007-5 Table R5 – System Access Control~~

Part	Applicable Systems	Requirements	Measures
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined

	Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA		number of unsuccessful login attempts.
~~Reference to prior version:~~ *~~New Requirement~~*		**~~Change Rationale:~~** *~~Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.~~*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~("~~" (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Violation Investigations

Self-Reporting

~~• Complaint~~

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.2) ~~OR~~ ~~The Responsible Entity has implemented and documented~~	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.1) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for determining~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R1) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)~~	~~necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)~~	~~the deficiencies. (R1)~~
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~6 Table R2 ~~and has identified deficiencies but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but~~	sources, for tracking or evaluating cyber security patches for applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or~~	applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and	~~not assess or correct the deficiencies~~. (R2)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2)~~ OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35	~~correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2)	implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for~~	security patches for applicable Cyber Assets~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but less than 50 calendar days of the evaluation completion ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation~~	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion ~~and has identified deficiencies but did not assess or correct~~	~~applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4) ~~OR~~ ~~The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess,~~	plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an~~	~~not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4)~~ OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4) ~~OR~~ ~~The Responsible Entity documented~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~or correct the deficiencies. (2.3)~~	~~existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)~~
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns~~ and has identified~~	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code~~ and has identified deficiencies but did not assess or correct~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R3 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~deficiencies but did not assess or correct the deficiencies~~. (3.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)~~	~~the deficiencies~~. (3.2)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used,	~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify, assess, or correct the deficiencies. (R3)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code~~ and has identified~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the Responsible Entity did not update malicious code protections ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (3.3)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies.~~ ~~(3.3)~~	~~deficiencies but did not assess or correct the deficiencies~~. (3.1) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies.~~ ~~(3.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the d~~	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4) ~~The Responsible Entity has documented and~~	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.2)~~OR~~ ~~The Responsible Entity has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R4 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R4)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4~~	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2)~~ OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.1) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log events for the~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.3) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional~~	~~Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3)~~OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals~~ and has identified deficiencies but did~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (4.4)~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)~~	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for~~	process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~The Responsible Entity has implemented one or more documented process(es) for password-only~~	process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the~~	more process(es) that included the applicable items in CIP-007-~~5~~6 Table R5 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R5) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5)~~OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2)~~OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts~~ and has identified deficiencies but did~~	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (5.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only	authentication of interactive user access~~ and did not identify, assess, or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.4) ~~OR~~ ~~The Responsible Entity has~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce	~~implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					one of the two password parameters as described in 5.5.1 and 5.5.2~~ and did not identify, assess, or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months	described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password~~	~~or correct the deficiencies. (5.5)~~ OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.7)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)~~

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

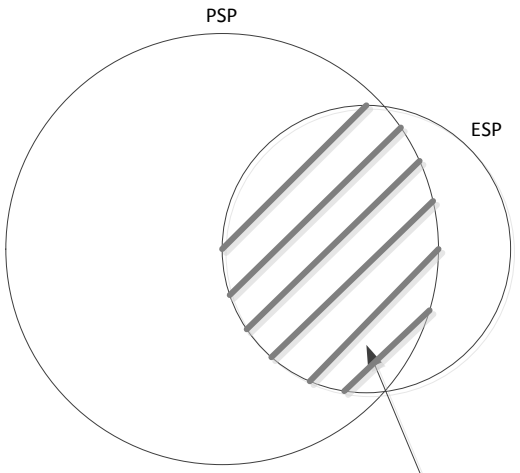
- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense ~~are~~is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. ~~Stand alone~~Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they

can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, ~~portable storage media policies,~~ Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc~~).~~.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted final ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-009-6.

6. Background:

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

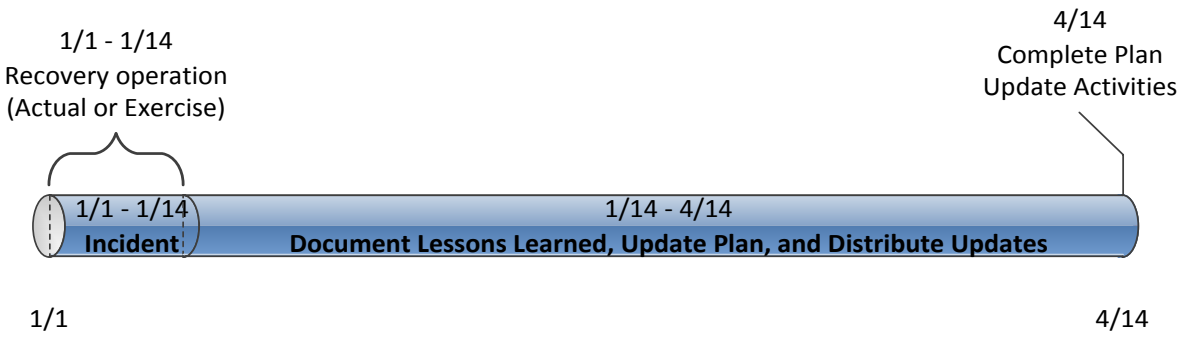


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

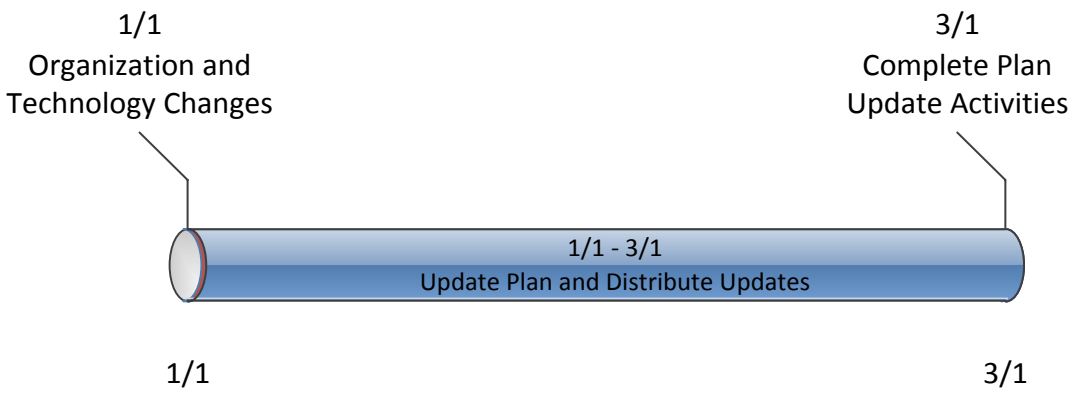


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014
~~3.~~4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted ~~for an additional comment and ballot~~final ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
~~Additional 45-Day Comment Period~~	~~August 2014~~
Final Ballot is Conducted	October~~/November~~ 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
~~6~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-009-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction~~See Implementation Plan for CIP-009-6.

6. Background:

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6~~5~~ Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants~~' facilities~~.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

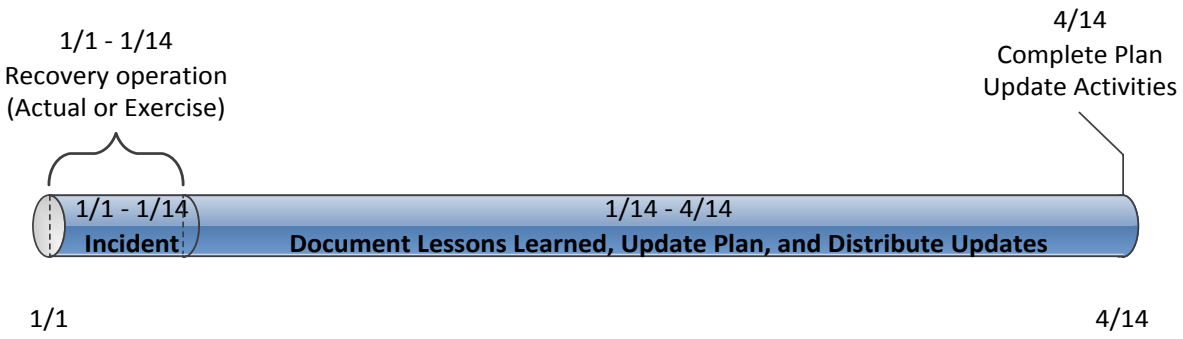


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

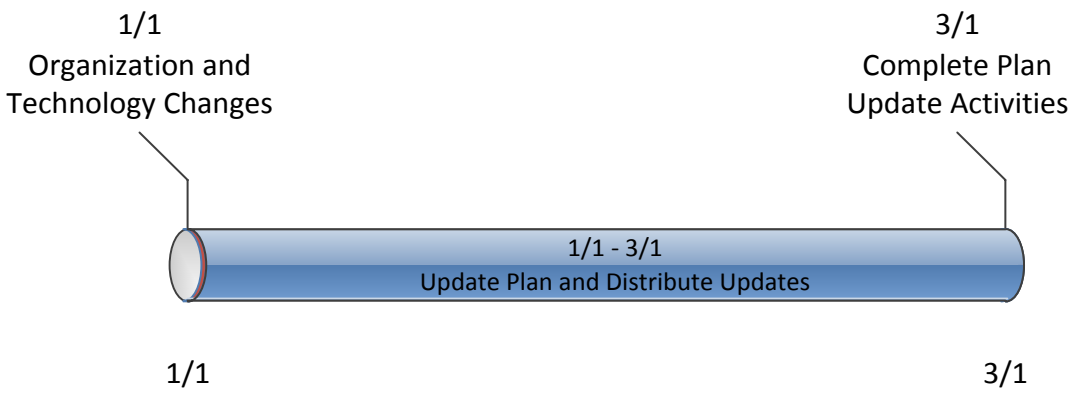


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment ~~(March 20, 2008).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014
3. First Comment and Ballot Period concluded on July 16, 2014
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted final ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014

~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014
~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

~~Effective Dates~~

1. ~~**24 Months Minimum –** CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~
2. ~~In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~".~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~Responsible Entity.~~responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated ~~version number~~Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	~~Update~~
3	3/31/10	Approved by FERC.	
4	~~12/30/10~~1/24/11	~~Modified to add specific criteria for Critical Asset identification.~~Approved by the NERC Board of Trustees.	~~Update~~
~~4~~5	~~1/24/~~11/26/12	~~Approved~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	~~TBD~~11/22/13	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~FERC Order issued approving CIP-009-5.	

~~Definitions of Terms Used in the Standard~~

~~*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*~~

When this standard has received ballot approval, the text boxes will be moved to the ~~"~~Application Guidelines ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-~~5~~6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-009-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-009-6.

6. Background:

Standard CIP-009 ~~-5~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~].~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~ **~~in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the~~

~~documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

~~**Rationale for R1:** Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

~~**Summary of Changes:** Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.~~

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery ~~plans~~plan(s) that collectively include each of the applicable requirement parts in *CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications*.

CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
~~**Reference to prior version:**~~ ~~*CIP-009, R1.1*~~		~~**Change Description and Justification:** *Minor wording changes; essentially unchanged.*~~	
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
~~**Reference to prior version:**~~ ~~*CIP-009, R1.2*~~		~~**Change Description and Justification:** *Minor wording changes; essentially unchanged.*~~	

CIP-009-~~5~~6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

~~Reference to prior version:~~ **CIP-009~~, R4~~-6 Table R1 – Recovery Plan Specifications**	~~**Change Description and Justification:** *Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.*~~

~~CIP-009-5 Table R1 – Recovery Plan Specifications~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*~~	
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

~~Reference to prior version:~~ ~~*New*~~**Rationale for Requirement R2:** The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans. Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.	**~~Change Description and Justification:~~** ~~*Added requirement to address FERC Order No. 706, Paragraph 706.*~~

~~**Rationale for R2:**~~

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

~~**Summary of Changes.** Added operational testing for recovery of BES Cyber Systems.~~

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
~~**Reference to prior version:**~~ ~~*CIP-009, R2*~~		~~**Change Description and Justification:** *Minor wording change; essentially unchanged.*~~	

CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
~~**Reference to prior version:**~~ ~~*CIP-009, R5*~~		~~**Change Description and Justification:** *Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.*~~	

CIP-009-~~5~~6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

~~Reference to prior version:~~ *~~CIP-009, R2~~*	**~~Change Description and Justification:~~** *~~Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.~~* **Rationale for Requirement R3:** To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

~~**Rationale for R3:** To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

~~**Summary of Changes:** Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.~~

R3. Each Responsible Entity shall maintain each of its recovery ~~plans~~plan(s) in accordance with each of the applicable requirement parts in *CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-~~5~~6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~**Reference to prior version:**~~ ~~*CIP-009, R1 and R3*~~		~~**Change Description and Justification:** *Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.*~~	
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~("~~" (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance ~~Investigation~~Investigations

Self-Reporting

~~• Complaint~~

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests~~, and~~	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests~~, and when tested, any~~	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests~~, and~~	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~when tested, any deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~when tested, any deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~OR~~ The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) ~~OR~~ ~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~deficiencies, but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)~~
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than ~~210~~ 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power ~~plants' facilities~~plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

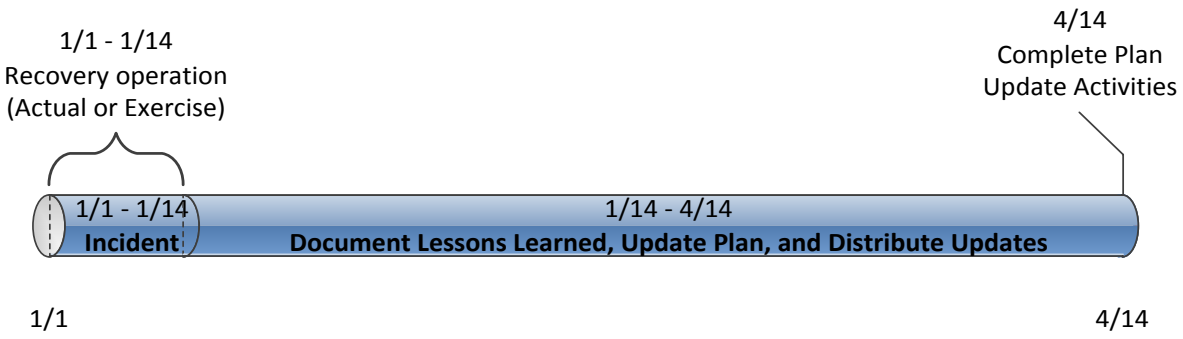


Figure 1: CIP-009-~~5~~6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

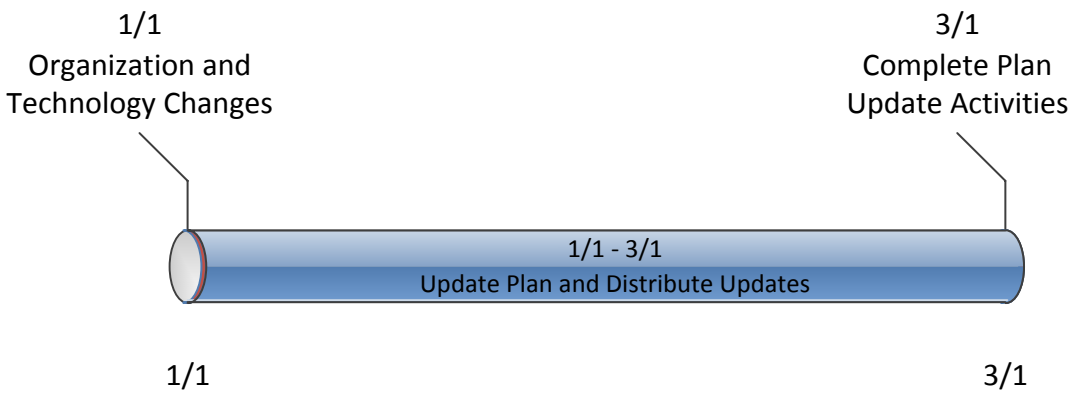


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.**~~

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. ~~3.~~ Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for ~~an additional comment and ballot to ballot the removal of "identify, assess, and correct" language~~final ballot. The draft includes modifications to meet the FERC Order No. 791 directive~~s to remove or modify the "identify, assess, and correct" language from CIP-010~~.

Anticipated Actions	Anticipated Date
~~Additional 45-Day Comment Period~~	~~September 2014~~
Final Ballot is Conducted	October~~/November~~ 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
~~X~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-~~X~~2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-~~X~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~Reliability Standard CIP-010-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction~~See Implementation Plan for CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~X~~ 2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~X~~ 2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~X~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~X~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~X~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~X~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~X~~ 2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~X~~ 2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~X~~ 2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~X~~ 2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~X~~ 2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~X~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~X~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~X~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment ~~(March 20, 2008).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014

~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014
~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

~~Effective Dates~~

1. ~~**24 Months Minimum –** CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~
2. ~~In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

Version History

Version	Date	Action	Change Tracking
1	~~TBD~~11/26/12	~~Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.~~Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	

~~Definitions of Terms Used in Standard~~

~~*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*~~

When this standard has received ballot approval, the text boxes will be moved to the ~~"~~Application Guidelines ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-~~1~~2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-010-2.

6. Background:

Standard CIP-010~~-1~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~].~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table. ~~The~~

~~documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk

Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS~~)~~ ~~–~~)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS~~)~~ ~~–~~)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

~~**Rationale – R1:**~~

~~The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.~~

- .

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~Reference to prior version:~~ ~~*New Requirement*~~		**~~Change Rationale:~~** ~~*The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*~~	
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
~~Reference to prior version:~~ ~~*CIP-007-3, R9; CIP-003-3, R6*~~		**~~Change Rationale:~~** ~~*The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*~~	

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
~~**Reference to prior version:**~~ ~~*CIP-007-3, R9; CIP-005-3, R5*~~		~~**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*~~	

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
~~**Reference to prior version:**~~ ~~*CIP-007-3, R1*~~		~~**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*~~	

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

~~**Reference to prior version:**~~ ~~*CIP-007-3, R1*~~	~~**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.*~~ ~~*This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*~~**Rationale for Requirement R2:** The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

~~**Rationale – R2:**~~

~~The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.~~

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated:	Monitor at least once every 35 calendar days for changes to the baseline	An example of evidence may include, but is not limited to, logs from a

CIP-010-~~1~~2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PCA	configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.*~~ ~~*This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.*~~ ~~*Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*~~	

~~**Rationale – R3:**~~

~~The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.~~

~~The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.~~

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented ~~processes~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.
~~**Reference to prior version:**~~ ~~*CIP-005-4, R4; CIP-007-4, R8*~~		~~**Change Rationale:** *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*~~	

CIP-010-~~1~~2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Rationale:**~~ ~~*FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*~~ ~~*As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*~~	

CIP-010-~~1~~2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Rationale:**~~ ~~*FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*~~	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

~~**Reference to prior version:**~~ ~~*CIP-005-3, R4.5; CIP-007-3, R8.4*~~	~~**Change Rationale:**~~ ~~*Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*~~

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~(""~~ (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

b. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance ~~Audit~~Audits

Self-~~Certification~~Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

~~• Complaint~~

Complaints

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified~~	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~	~~identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required~~	~~deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for~~	~~implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify,~~	~~security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1)~~	~~changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update~~	update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~assess, or correct the deficiencies in the verification documentation. (1.4.3)~~		~~baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess,~~	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required~~	from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~the deficiencie (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~environments and identified deficiencies but did not assess or correct the deficiencies. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)~~OR~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)~~
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-~~5~~6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-~~5~~6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 ~~R1~~Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-011-2.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity

must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note: The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X standards were redlined to the industry-approved version 5 language for ease of reading revisions.**~~

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. ~~3.~~ Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

This draft standard is being posted for ~~an additional comment and ballot to ballot the removal of "identify, assess, and correct" language~~final ballot. The draft includes modifications to meet the FERC Order No. 791 directives~~ to remove or modify the "identify, assess, and correct" language from CIP-011~~.

Anticipated Actions	Anticipated Date
~~Additional 45-Day Comment Period~~	~~September 2014~~
Final Ballot is Conducted	October~~/November~~ 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
~~X~~	~~June 2014~~	~~Responding to FERC Order No. 791.~~	~~Revised~~

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~X~~2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~X~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

~~Reliability Standard CIP-011-X shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction~~See Implementation Plan for CIP-011-2.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~X~~ 2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~X~~ 2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~X~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~X~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~X~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~X~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~X~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-~~X~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~X~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity

must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment ~~(March 20, 2008).~~on January 15, 2014

~~2. SC authorized moving the SAR forward to standard development (July 10, 2008).~~

~~3. First posting for 60-day formal comment period and concurrent ballot (November 2011).~~

~~4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).~~

~~5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).~~

2. Standard Drafting Team appointed on January 29, 2014
3. First 45-Day Comment and Ballot Period concluded on July 16, 2014 with all revisions addressing FERC No. 791 directives
4. Additional 45-Day Comment Period and Ballot concluded on October 17, 2014

Description of Current Draft

~~This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.~~

This draft standard is being posted for final ballot. The draft includes modifications to meet the FERC Order No. 791 directives.

Anticipated Actions	Anticipated Date
Final Ballot is Conducted	October 2014
~~Recirculation ballot~~Board of Trustees (Board) Adoption	November ~~2012~~2014

~~BOT adoption~~Filing to Applicable Regulatory Authorities	December ~~2012~~2014

~~Effective Dates~~

1. ~~**24 Months Minimum –** CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~
2. ~~In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

Version History

Version	Date	Action	Change Tracking
1	~~TBD~~11/26/12	~~Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.~~Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	

~~Definitions of Terms Used in Standard~~

~~*See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.*~~

When this standard has received ballot approval, the text boxes will be moved to the ~~"~~Application Guidelines ~~and Technical Basis" section~~Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~1~~2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-011-2.

6. Background:

Standard CIP-011~~-1~~ exists as part of a suite of CIP Standards related to cyber security~~. CIP-002-5 requires~~, which require the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1,~~ and ~~CIP-011-1~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~.~~.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

> ~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~it must address the applicable requirements in the table~~. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the~~

~~documented processes and could be accomplished through other controls or compliance management activities~~.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA~~)~~) –** Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

- .

~~Rationale – R1:~~

~~The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

~~Summary of Changes: CIP-003-4 R4, R4.2, and R 4.3 have been moved to CIP-011 R1.~~
~~CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System~~

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~1~~2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~1~~2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~1~~2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~**Reference to prior version:**~~ ~~*CIP-003-3, R4; CIP-003-3, R4.2*~~		~~**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (*~~e.g., confidential, public, internal use only, etc.~~*) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*~~	

CIP-011-~~1~~2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

~~**Reference to prior version:**~~ ~~*CIP-003-3, R4;*~~	~~**Change** **Rationale:**~~ **for Requirement R2:** The ~~*SDT changed*~~intent of the ~~*language from "protect" information to "Procedures for protecting*~~BES Cyber Asset reuse and ~~*securely handling"*~~disposal process is to ~~*clarify*~~prevent the ~~*protection that is required*~~unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

~~**Rationale – R2:**~~

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

R2. Each Responsible Entity shall implement one or more documented ~~processes~~process(es) that collectively include the applicable requirement parts in *CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

~~**Reference to prior version:**~~ ~~*CIP-007-3, R7.2*~~CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal	~~**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*~~

~~CIP-011-1 Table R2 — BES Cyber Asset Reuse and Disposal~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.
~~**Reference to prior version:**~~ ~~*CIP-007-3, R7.1*~~		~~**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*~~ ~~*The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority ~~("~~" (CEA~~") unless~~) means NERC or the ~~applicable entity is owned, operated, or controlled by~~Regional Entity in their respective roles of monitoring and enforcing compliance with the ~~Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA~~NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance ~~Audit~~Audits
- Self-~~Certification~~Certifications
- Spot Checking
- Compliance ~~Investigation~~Violation Investigations
- Self-Reporting
- ~~Complaint~~
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify,~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~assess, or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~but did not identify, assess, or correct the deficiencies. (1.2)~~	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~1~~2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-~~5's~~5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity

must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

October 28, 2014

This Implementation Plan is a combination of the effective dates for CIP-006-6 and CIP-009-6 from the initial ballot and the effective dates for the version X standards from the additional ballot. This Implementation Plan does not apply to standards revised to address the "Low Impact" and "Transient Device" directives from FERC Order No. 791. Those revisions require additional development and will be addressed in future versions of the standards with an associated Implementation Plan.

Requested Approvals

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel & Training
- CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5.1 — Cyber Security — Personnel & Training
- CIP-006-5 — Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management and Vulnerability Assessments

- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

None

Effective Dates

The effective dates for each of the proposed Reliability Standards are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date that entities must begin to comply with that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-6 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-003-6, Requirement R2

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

2. CIP-004-6 — Cyber Security — Personnel & Training

   Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems

   Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-006-6, Requirement R1, Part 1.10

   For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-6 —Cyber Security — Systems Security Management

   Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on

the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems

Reliability Standard CIP–009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

7. CIP-011-2 — Cyber Security — Information Protection

Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where

approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. Standards for Retirement

CIP-003-5 shall retire at midnight of the day immediately prior to the effective date of CIP-003-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-004-5.1 shall retire at midnight of the day immediately prior to the effective date of CIP-004-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-006-5 shall retire at midnight of the day immediately prior to the effective date of CIP-006-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-007-5 shall retire at midnight of the day immediately prior to the effective date of CIP-007-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-009-5 shall retire at midnight of the day immediately prior to the effective date of CIP-009-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-010-1 shall retire at midnight of the day immediately prior to the effective date of CIP-010-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-011-1 shall retire at midnight of the day immediately prior to the effective date of CIP-011-2 in the particular jurisdiction in which the new standard is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[1] (Version 5 Plan) remain the same:

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.

- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[1] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

~~September 3, 2014~~October 28, 2014

Requested Approvals

- CIP-003-~~X~~ 6 — Cyber Security — Security Management Controls
- CIP-004-~~X~~ 6 — Cyber Security — Personnel ~~and~~& Training
- CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-~~X~~ 6 — Cyber Security — Systems Security Management
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-~~X~~ 2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-~~X~~ 2 — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5.1 — Cyber Security — Personnel ~~and~~& Training
- CIP-006-5 — Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management and Vulnerability Assessments

This Implementation Plan is a combination of the effective dates for CIP-006-6 and CIP-009-6 from the initial ballot and the effective dates for the version X standards from the additional ballot. This Implementation Plan does not apply to standards revised to address the "Low Impact" and "Transient Device" directives from FERC Order No. 791. Those revisions require additional development and will be addressed in future versions of the standards with an associated Implementation Plan. ~~**The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X implementation plan is posted in a clean version although it draws upon the implementation plan from the previous posting and only includes language for those standards balloted as version X.**~~

- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

None

~~**General Considerations**~~

~~The results of the initial CIP V5 Revisions ballot showed industry support for the new communication networks requirements and the removal of the identify, assess, and correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015.~~

~~The CIP-003-6 and CIP-010-2 revisions proposed to address the low impact and transient devices directives did not pass initial ballot. As a prudent approach and in order to meet the FERC filing deadline of February 3, 2015 for the two directives, the SDT would like to ballot the IAC revisions on their own without the low impact and transient devices revisions. Assuming the IAC revisions pass the second ballot, these standards can proceed to final ballot along with the communication networks revisions.~~

~~The SDT emphasizes that this is NOT an indication that it plans to separate the revision work. Strong progress continues on the low impact and transient devices revisions, and the SDT still hears support from stakeholders to complete all four directive areas of FERC Order No. 791 revisions at the same time. The request for a separate ballot is a practical measure to avoid potential complications with meeting FERC's directive deadlines that, if we were to wait until after the second ballot, time may not allow us to address.~~

~~The SDT plans to post a single ballot for the standards that need stakeholder approval for the IAC language removal. These proposed standards will be version X for the ballot. The version X ballot will be posted along with the other revision proposals designated with the appropriate version number. This allows for the simultaneous revision of the standards to address the directive issue areas and when both the version X and the numbered version standards pass ballot, the revisions can be combined into the appropriate numbered standard version.~~

Effective Dates

The effective dates for each of the proposed Reliability Standards ~~and NERC Glossary terms~~ are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date that entities must begin to comply with that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-~~X~~ 6 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-~~X~~ 6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-003-~~X~~6, Requirement R2

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-~~X~~6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-~~X~~6.

2. CIP-004-~~X~~ 6 — Cyber Security — Personnel ~~and~~& Training

   Reliability Standard CIP-004-~~X~~ 6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-006-6, Requirement R1, Part 1.10

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

~~3.~~4. CIP-007-~~X~~6 —Cyber Security — Systems Security Management

Reliability Standard CIP-007-~~X~~6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-~~X~~6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-~~X~~6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-~~X~~6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems

Reliability Standard CIP–009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

~~4.~~6. CIP-010-~~X~~ 2 — Cyber Security — Configuration Change Management and Vulnerability Assessments

Reliability Standard CIP-010-~~X~~ 2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

~~5.~~7. CIP-011-~~X~~ 2 — Cyber Security — Information Protection

Reliability Standard CIP-011-~~X~~ 2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

~~6.~~8. Standards for Retirement

~~Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.~~

CIP-003-5 shall retire at midnight of the day immediately prior to the effective date of CIP-003-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-004-5.1 shall retire at midnight of the day immediately prior to the effective date of CIP-004-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-006-5 shall retire at midnight of the day immediately prior to the effective date of CIP-006-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-007-5 shall retire at midnight of the day immediately prior to the effective date of CIP-007-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-009-5 shall retire at midnight of the day immediately prior to the effective date of CIP-009-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-010-1 shall retire at midnight of the day immediately prior to the effective date of CIP-010-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-011-1 shall retire at midnight of the day immediately prior to the effective date of CIP-011-2 in the particular jurisdiction in which the new standard is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[1] (Version 5 Plan) remain the same:

- *Initial Performance of Certain Periodic Requirements*

- For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.

- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

For *unplanned* changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

[1] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791

October 28, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section

[2] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 186, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	1600 data request and will be working with the six study participants in developing the information needed for its filing.
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to the CIP version 5 Standards.4 The Commission agrees	NERC modified the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[3] *See infra* P 223.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5,	NERC modified the VRF assignment for CIP-004-5.1, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-5, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		2. **VSLs for CIP-004-5.1, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-5, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the timeframe contained in the VSLs from 90-210 days to 90-120 days.

Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791

~~September 3, 2014~~October 28, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
~~106~~	~~Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact~~	~~The SDT revised Requirements R1 and R2 of CIP-003-6 to include additional specificity regarding the processes that responsible entities must have for low impact BES Cyber Systems. In addition, the SDT developed objective criteria~~

[2] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 186, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	~~facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.~~	~~surrounding the controls for some entities based on asset type and routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category.~~ ~~To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility site level.~~ ~~The SDT confined these revisions in CIP-003-6, Requirements R1 and R2 to the following areas:~~ ~~1. **Cyber Security Policy:** R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan.~~ ~~2. **Cyber Security Plan(s):** R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s). The cyber security plan must cover the 4 areas as~~

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		~~specified in Attachment 1 of CIP-003-6:~~ ~~a. **Cyber Security Awareness:** Attachment 1, element 1 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices. The SDT determined that adding intervals increases the auditability of the requirement part.~~ ~~b. **Physical Security Controls:** Attachment 1, element 2 and its subparts require controls to restrict physical access to low impact BES Cyber Systems as well as Low Impact BES Cyber System Electronic Access Points (LEAP) used for controlling access as specified in element 3.~~ ~~c. **Electronic Access Controls:** Attachment 1, element 3 and its subparts address protections around Low Impact BES Cyber System External Routable Connectivity (LERC) and Dial-up Connectivity.~~ ~~d. **Cyber Security Incident Response:** Attachment 1, element 4 and its subparts outline the criteria required to be in a Cyber Security Incident response plan.~~

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing.
~~132~~	~~Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it would be unduly burdensome for responsible entities~~	~~The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which requires a Transient Cyber Asset and Removable Media plan to provide higher assurance against the propagation of malware when connecting transient devices.~~

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	~~to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.~~	~~The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition.~~ ~~The drafting team determined three distinct scenarios for entities to address in their plan(s) in which transient devices need specific protections: (i) Transient Cyber Assets owned or managed by the Responsible Entity, (ii) Transient Cyber Asset(s) owned or managed by vendors or contractors, and (iii) Removable Media.~~ ~~For Transient Cyber Assets owned or managed by the Responsible Entity, the SDT determined that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management. The controls for this scenario are more specific and recognize the relatively higher frequency in which these devices will be used.~~

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		~~In the scenario in which contractors or vendors manage the Transient Cyber Assets, the required elements of the plan include those which an entity can verify at the point prior to connecting such as security patch management and malware prevention mechanisms.~~ ~~The security controls entities must apply to Removable Media have considerations for the type of device being protected and include authorization and scanning for malicious code.~~ ~~The Commission provided a list of security controls it expected NERC to consider for addressing transient devices. The consideration of each security element is described as follows:~~ ~~1. **Device authorization as it relates to users and locations:** CIP-010-2 Requirement R4, Attachment 1 requires entities to authorize Transient Cyber Assets and Removable Media by individual(s) and location(s) prior to connecting them to the BES Cyber System. Vendor or contractor managed Transient Cyber Assets do not have this authorization because the scenario is often single-use and the entity already conducts an inspection and mitigation of the device prior to connection.~~ ~~2. **Software authorization:** The SDT considered controls relating to software authorization but decided against including specific software as part of the authorization performance because such authorization did not~~

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		~~contribute meaningfully to cyber security risk reduction. However, software authorization in the form of application whitelisting is provided as an option to mitigate malicious code.~~ ~~3. **Security patch management:** In CIP-010-2 R4, Attachment 1, both entity and vendor/contractor managed devices must have security patch management or other equivalent forms of mitigation to address security vulnerabilities in software.~~ ~~4. **Malware prevention:** CIP-010-2 Requirement R4, Attachment 1 requires entities to have malware protection on the Transient Cyber Asset (for both entity- and vendor-managed Transient Cyber Assets) and for Removable Media prior to connection.~~ ~~5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this control and determined this control best applies to entity-managed Transient Cyber Assets with the objective to mitigate the risk of unauthorized use. There are logistical challenges in applying this control to vendor-managed devices, in which the entity likely will have had no control until immediately prior to use. Furthermore, additional guidance is necessary in CIP-011-2 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		~~devices. The objective to address the unauthorized release of BES Cyber System Information is sufficiently addressed with the requirements in CIP-011-2 to protect and securely handle BES Cyber System Information.~~ ~~6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-2 requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-2 Requirement R4.~~
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.
181 and 184	181. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move	NERC modified the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[3] *See infra* P 223.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	from compliance with the CIP version 3 Standards to the CIP version 5 Standards.4 The Commission agrees that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment	NERC modified the VRF assignment for CIP-004-5.1, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-5, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language. 2. **VSLs for CIP-004-5.1, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-5, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		timeframe contained in the VSLs from 90-210 days to 90-120 days.

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 (CIP-002-5, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-6 R1	No change.
CIP-003-5 R1.1	CIP-003-6 R1.1	No change.
CIP-003-5 R1.2	CIP-003-6 R1.2	No change.
CIP-003-5 R1.3	CIP-003-6 R1.3	No change.
CIP-003-5 R1.4	CIP-003-6 R1.4	No change.
CIP-003-5 R1.5	CIP-003-6 R1.5	No change.
CIP-003-5 R1.6	CIP-003-6 R1.6	No change.
CIP-003-5 R1.7	CIP-003-6 R1.7	No change.
CIP-003-5 R1.8	CIP-003-6 R1.8	No change.
CIP-003-5 R1.9	CIP-003-6 R1.9	No change.
CIP-003-5 R2	CIP-003-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.1	CIP-003-6 R2.1	No change.
CIP-003-5 R2.2	CIP-003-6, R2.2	No change.
CIP-003-5 R2.3	CIP-003-6 R2.3	No change.
CIP-003-5 R2.4	CIP-003-6 R2.4	No change.
CIP-003-5 R3	CIP-003-6 R3	No change.
CIP-003-5 R4	CIP-003-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-6 R1	No change.
CIP-004-5.1 R1.1	CIP-004-6 R1.1	No change.
CIP-004-5.1 R2	CIP-004-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R2.1	CIP-004-6 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-6 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-6 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-6 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-6 R2.1.4	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.1.5	CIP-004-6 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-6 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-6 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-6 R2.1.8	No change.
CIP-004-5.1 R2.2	CIP-004-6 R2.2	No change.
CIP-004-5.1 R2.3	CIP-004-6 R2.3	No change.
CIP-004-5.1 R3	CIP-004-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R3.1	CIP-004-6 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-6 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-6 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-6 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-6 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-6 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-6 R3.5	No change.
CIP-004-5.1 R4	CIP-004-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R4.1	CIP-004-6 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-6 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-6 R4.1.2	No change.
CIP-004-5.1 R4.1.3	CIP-004-6 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-6 R4.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R4.3	CIP-004-6 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-6 R4.4	No change.
CIP-004-5.1 R5	CIP-004-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R5.1	CIP-004-6 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-6 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-6 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-6 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-6 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-6 R1.1	No change.
CIP-007-5 R1.2	CIP-007-6 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-6 R2.1	No change.
CIP-007-5 R2.2	CIP-007-6 R2.2	No change.
CIP-007-5 R2.3	CIP-007-6 R2.3	No change.
CIP-007-5 R2.4	CIP-007-6 R2.4	No change.
CIP-007-5 R3	CIP-007-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.1	CIP-007-6 R3.1	No change.
CIP-007-5 R3.2	CIP-007-6 R3.2	No change.
CIP-007-5 R3.3	CIP-007-6 R3.3	No change.
CIP-007-5 R4	CIP-007-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R4.1	CIP-007-6 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-6 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-6 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-6 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-6 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-6 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-6 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-6 R4.3	No change.
CIP-007-5 R4.4	CIP-007-6 R4.4	No change.
CIP-007-5 R5	CIP-007-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R4	CIP-007-6 R4	No change.
CIP-007-5 R5	CIP-007-6 R5	No change.
CIP-007-5 R5.1	CIP-007-6 R5.1	No change.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R5.4	CIP-007-6 R5.4	No change.
CIP-007-5 R5.5	CIP-007-6 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-6 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-6 R5.5.2	No change.
CIP-007-5 R6	CIP-007-6 R6	No change.
CIP-007-5 R7	CIP-007-6 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-2 R1.1	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-2 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-2 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-2 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-2 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-2 R1.5.2	No change.
CIP-010-1 R2	CIP-010-2 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-2 R2.1	No change.
CIP-010-1 R3	CIP-010-2 R3	No change.
CIP-010-1 R3.1	CIP-010-2 R3.1	No change.
CIP-010-1 R3.2	CIP-010-2 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-2 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-2 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-2 R3.3	No change.
CIP-010-1 R3.4	CIP-010-2 R3.4	No change.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-2 R1.1	No change.
CIP-011-1 R1.2	CIP-011-2 R1.2	No change.
CIP-011-1 R2	CIP-011-2 R2	No change.
CIP-011-1 R2.1	CIP-011-2 R2.1	No change.
CIP-011-1 R2.2	CIP-011-2 R2.2	No change.

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 (CIP-002-5, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-6 R1	~~To incorporate a policy or policies for low impact BES Cyber Systems, the main requirement language was modified. "For its high impact and medium impact BES Cyber Systems" was struck from the language as new requirement parts were created. See below for part 1.1 and part 1.2 to see the change justification.~~No change.
~~NEW~~	~~CIP-003-6 R1.1~~	~~"For its high impact and medium impact BES Cyber Systems" was added as a qualifier to the sub-parts below.~~
CIP-003-5 R1.1	CIP-003-6 R1.1~~.1~~	~~Requirement parts for 1.1 through 1.9 have become 1.1.1 through 1.1.9 with the clarifier added above in part 1.1 of CIP-003-6.~~ No change.
CIP-003-5 R1.2	CIP-003-6 R1.~~1.~~2	No change.
CIP-003-5 R1.3	CIP-003-6 R1.~~1.~~3	No change.
CIP-003-5 R1.4	CIP-003-6 R1.~~1.~~4	No change.
CIP-003-5 R1.5	CIP-003-6 R1.~~1.~~5	No change.
CIP-003-5 R1.6	CIP-003-6 R1.~~1.~~6	No change.
CIP-003-5 R1.7	CIP-003-6 R1.~~1.~~7	No change.
CIP-003-5 R1.8	CIP-003-6 R1.~~1.~~8	No change.
CIP-003-5 R1.9	CIP-003-6 R1.~~1.~~9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
~~NEW~~	~~CIP-003-6 R1.2~~	~~"For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:" was added as a qualifier to the sub-parts below.~~
CIP-003-5 R2	CIP-003-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. ~~Furthermore, as the SDT modified its approach of using Attachment 1 instead of the table approach, it modified Requirement R2 to "implement one or more document cyber security plan(s) that include the applicable elements in Attachment 1."~~
CIP-003-5 R2.1	CIP-003-6 R~~1.2.1~~2.1	~~The security awareness requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.1~~No change.
CIP-003-5 R2.2	CIP-003-6, R~~1.2.2~~2.2	~~The physical security controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.2.~~No change.
CIP-003-5 R2.3	CIP-003-6 R~~1.2.3~~2.3	~~The electronic access controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.3. Furthermore, the SDT modified the "external routable protocol connections" as a new definition is being proposed by the SDT for "Low Impact External Routable Connectivity."~~ No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.4	CIP-003-6 R~~1.2.4~~2.4	~~The incident response to a Cyber Security Incident requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.4.~~ No change.
~~NEW~~	~~CIP-003-6, Attachment 1~~	~~CIP-003-6 Attachment 1 lists the elements required for low impact asset cyber security plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the lack of objective criteria for Low Impact assets protections.~~
CIP-003-5 R3	CIP-003-6 R3	No change.
CIP-003-5 R4	CIP-003-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-6 R1	No change.
CIP-004-5.1 R1.1	CIP-004-6 R1.1	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2	CIP-004-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. ~~The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement "a cyber security training program(s)." That modification was made for clarity and consistency across the standards.~~
CIP-004-5.1 R2.1	CIP-004-6 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-6 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-6 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-6 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-6 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-6 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-6 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-6 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-6 R2.1.8	No change.
~~CIP-004-5.1 R2.1.9~~	~~CIP-004-6 R2.1.9~~	~~To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity's cyber security training program. The training must address cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.~~
CIP-004-5.1 R2.2	CIP-004-6 R2.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.3	CIP-004-6 R2.3	No change.
CIP-004-5.1 R3	CIP-004-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R3.1	CIP-004-6 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-6 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-6 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-6 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-6 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-6 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-6 R3.5	No change.
CIP-004-5.1 R4	CIP-004-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R4.1	CIP-004-6 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-6 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-6 R4.1.2	No change.
CIP-004-5.1 R4.1.3	CIP-004-6 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-6 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-6 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-6 R4.4	No change.
CIP-004-5.1 R5	CIP-004-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R5.1	CIP-004-6 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-6 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-6 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-6 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-6 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-6 R1.1	No change.
CIP-007-5 R1.2	CIP-007-6 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection again the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-6 R2.1	No change.
CIP-007-5 R2.2	CIP-007-6 R2.2	No change.
CIP-007-5 R2.3	CIP-007-6 R2.3	No change.
CIP-007-5 R2.4	CIP-007-6 R2.4	No change.
CIP-007-5 R3	CIP-007-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R3.1	CIP-007-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.2	CIP-007-6 R3.2	No change.
CIP-007-5 R3.3	CIP-007-6 R3.3	No change.
CIP-007-5 R4	CIP-007-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R4.1	CIP-007-6 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-6 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-6 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-6 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-6 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-6 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-6 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-6 R4.3	No change.
CIP-007-5 R4.4	CIP-007-6 R4.4	No change.
CIP-007-5 R5	CIP-007-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R4	CIP-007-6 R4	No change.
CIP-007-5 R5	CIP-007-6 R5	No change.
CIP-007-5 R5.1	CIP-007-6 R5.1	No change.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.4	CIP-007-6 R5.4	No change.
CIP-007-5 R5.5	CIP-007-6 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-6 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-6 R5.5.2	No change.
CIP-007-5 R6	CIP-007-6 R6	No change.
CIP-007-5 R7	CIP-007-6 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-2 R1.1	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-2 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-2 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-2 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-2 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-2 R1.5.2	No change.
CIP-010-1 R2	CIP-010-2 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-2 R2.1	No change.
CIP-010-1 R3	CIP-010-2 R3	No change.
CIP-010-1 R3.1	CIP-010-2 R3.1	No change.
CIP-010-1 R3.2	CIP-010-2 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-2 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-2 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-2 R3.3	No change.
CIP-010-1 R3.4	CIP-010-2 R3.4	No change.
~~NEW~~	~~CIP-010-2 R4~~	~~To respond to the FERC Order No. 791 directive to address transient devices, the SDT modified its approach to use Attachment 1 instead of the table approach. It modified Requirement R4 to "implement one or more documented plan(s) for Transient Cyber Asset and Removable Media that include the applicable elements in Attachment 1, except under CIP Exceptional Circumstances."~~
~~NEW~~	~~CIP-010-2, Attachment 1~~	~~CIP-010-2 Attachment 1 lists the elements required for Transient Cyber Asset and Removable Media Plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the risks posed by transient devices.~~

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-2 R1.1	No change.
CIP-011-1 R1.2	CIP-011-2 R1.2	No change.
CIP-011-1 R2	CIP-011-2 R2	No change.
CIP-011-1 R2.1	CIP-011-2 R2.1	No change.
CIP-011-1 R2.2	CIP-011-2 R2.2	No change.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02 - Cyber Security - Order No. 791 Identify, Assess, and Correct and Communication Networks Directives

Violation Risk Factor and Violation Severity Level Justifications

The tables in this document provide a working draft of the analysis and justification for each Violation Risk Factor (VRF) and Violation Severity Level (VSL) for each requirement in the CIP Cyber Security Standards revisions that address the Order No. 791 identify, assess, and correct and communication networks directives.

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

The CIP Version 5 Revisions Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria – VRFs

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC VRF Guidelines

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the VRF Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria - VSLs

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on the guidelines shown in the table below:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital Component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC Orders on VSLs

In its June 19, 2008 Order on VSLs, FERC indicated it would use the following four guidelines for determining whether to approve VSLs:

Guideline 1: VSL Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

- Compare the VSLs to any prior Levels of Non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when Levels of Non-compliance were used.

Guideline 2: VSL Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

- Guideline 2a: A violation of a "binary" type requirement must be a "Severe" VSL.
- Guideline 2b: Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: VSL Assignment Should Be Consistent with the Corresponding Requirement

- VSLs should not expand on what is required in the requirement.

Guideline 4: VSL Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

In its March 18, 2010 Order Addressing VSL Assignments in CIP Standards, FERC offered the following additional guidance relative to VSLs for CIP requirements:

Guideline 5: Requirements Where Single Lapse in Protection Result in Compromised Computer Network Security

Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary rather than gradated Violation Severity Levels.

Guideline 6: VSLs Should Account for Interdependent Tasks

Violation Severity Levels for cyber security Requirements containing interdependent tasks of documentation and implementation should account for their interdependence.

VRF and VSL Justifications – CIP-003-6, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Security policies enable effective implementation of the CIP standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. However, given the scoping of the this requirement to only those BES assets that contain low impact BES Cyber Systems, a VRF of Lower was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security policy that contains certain elements specified in the requirement. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of elements, not necessarily parts, that must be included in the cyber security policy, the VRF is reflective of the policy as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards.

VRF and VSL Justifications – CIP-003-6, R2			
	This requirement maps from CIP-003-5, R1, which has an approved VRF of Lower but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security policy would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security policy requirement encompasses a number of policy domains. The VRF is identified at the risk level represented by all of the policy domains in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low	The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low

VRF and VSL Justifications – CIP-003-6, R2			
security policies for assets with a low impact rating as required by Requirement R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	security policies for assets with a low impact rating as required by Requirement R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	impact rating as required by Requirement R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	impact rating as required by Requirement R2 within 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2 by the CIP Senior Manager within 18 calendar months of the previous approval. (R2)

VRF and VSL Justifications – CIP-003-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-003-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-003-6, R2	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.

VRF and VSL Justifications – CIP-003-6, R2	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one or more of the required topics. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-6, R4	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability purpose of this requirement is to ensure clear lines of authority and ownership for security matters that could impact the stability and integrity of the Bulk Electric System, that delegations are kept up-to-date, and that individuals do not assume undocumented authority. As this requirement is only a part of the overall governance structure of a cyber security program, which includes additional leadership and policy, a VRF of Lower was assigned to this requirement.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement directs that the CIP Senior Manager is responsible for all approval and authorizations, but also grants the CIP Senior Manager with the ability to delegate this authority. The Requirement also calls for changes to the CIP Senior Manager and any delegations to be documented within 30 calendar days. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The requirement does not contain parts and are, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-003-5, R4, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to show clear authorization for actions taken back to the CIP Senior Manager would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The obligation of this requirement is to demonstrate that the CIP Senior Manager is ultimately responsible for all approvals and authorizations required in the CIP Standards. This requirement allows for delegation, but also obligates the Responsible Entity to document these delegations. The VRF was chosen based upon the highest reliability risk objective, which is the clear line of authority to the CIP Senior Manager and are, therefore, consistent with VRF Guideline 5.

VRF and VSL Justifications – CIP-003-6, R4			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

VRF and VSL Justifications – CIP-003-6, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. There is a single element upon which severity may be gradated; as such, gradated VSLs were assigned.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-003-5 R4. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-003-6, R4	
Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The requirement contains interdependent tasks of documentation and implementation. The VSL requirement presumes that the only way to demonstrate compliance is through documentation; as such, the VSLs are based upon the documentation measure, and implementation is assumed with documentation, therefore accounting for the interdependence in these tasks.

VRF and VSL Justifications – CIP-004-6, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective would not have adverse effect on the electrical state or capability of the Bulk Electric System.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-5.1, R2, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a training program would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity implemented a cyber security training program but failed to include one of	The Responsible Entity implemented a cyber security training program but failed to include two of the training	The Responsible Entity implemented a cyber security training program but failed to include three of the training	The Responsible Entity did not implement a cyber security training program appropriate to

VRF and VSL Justifications – CIP-004-6, R2			
the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals

VRF and VSL Justifications – CIP-004-6, R2			
			with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)

VRF and VSL Justifications – CIP-004-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-004-6, R2	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation,	The VSLs are based on a single violation and not cumulative violations.

VRF and VSL Justifications – CIP-004-6, R2	
Not on A Cumulative Number of Violations	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This VSL accounts for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation.

VRF and VSL Justifications – CIP-004-6, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.

VRF and VSL Justifications – CIP-004-6, R3	
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for implementing a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the Requirement level and the requirement parts are treated equally. Each Requirement Part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-5.1, R2, which has an approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a security training program could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining

VRF and VSL Justifications – CIP-004-6, R3			
physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR	physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical	authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR

VRF and VSL Justifications – CIP-004-6, R3			
The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or

VRF and VSL Justifications – CIP-004-6, R3			
			more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)

VRF and VSL Justifications – CIP-004-6, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R3. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations. The requirement is to implement a training program and failure for a single individual to have training does not necessarily imply a single violation. An overall view of the training program must consider the number of individuals who failed to receive training for a given period.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security. Although failure to implement a training program could associatively affect the ways in which computer network security applies, it does not, by itself, indicate a failure of computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This Requirement pertains to implementing the cyber security program and does not require procedural documentation.

VRF and VSL Justifications – CIP-004-6, R4			
Proposed VRF	**LOWER**		
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have received a personnel risk assessment. Failure to meet this objective could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for a personnel risk assessment program for individuals needing or having access to a BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement's VRF is consistent with similar security requirements with similar risks in the other CIP standards.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a personnel risk assessment program could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that documentation a personnel risk assessment is developed for individuals with access to BES Cyber Systems and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter	The Responsible Entity did not implement any documented program(s) for access management. (R4)

VRF and VSL Justifications – CIP-004-6, R4			
during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and	during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar	but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage	OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

VRF and VSL Justifications – CIP-004-6, R4			
necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary. (4.4)	months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	locations, privileges were incorrect or unnecessary. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

VRF and VSL Justifications – CIP-004-6, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R4. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document or implement all required documented program(s) has a binary Severe VSL. Other Requirement Parts associated with the required processes do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-004-6, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Failure to revoke access to BES Cyber Systems and BES Cyber System Information within the required time frame is an administrative requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to revoke access to BES Cyber Systems and BES Cyber System Information when individuals no longer need access. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. Each Requirement row contributes to the objective of this Requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-5.1, R5, which has an approved VRF of Medium. Therefore, the proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to revoke access to BES Cyber Systems and BES Cyber System Information may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this Requirement, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Requirement R5 requires prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Each part of Requirement R5 specifies the obligations to revoke access in various situations when an individual no longer needs such access.

VRF and VSL Justifications – CIP-004-6, R5			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following

VRF and VSL Justifications – CIP-004-6, R5			
The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)	day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

VRF and VSL Justifications – CIP-004-6, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R5. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R5	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to implement programs for access revocation has a binary Severe VSL. A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-006-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this Requirement. The requirement specifies that each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. Failure to restrict physical access to BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets could result in unauthorized access, which could directly affect the ability to monitor or control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-5, R1, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-6, R1 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-006-6, Requirement R1 requires the implementation of documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. A failure to implement these documented plans may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this requirement,

VRF and VSL Justifications – CIP-006-6, R1			
	if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2)

VRF and VSL Justifications – CIP-006-6, R1			
			OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each

VRF and VSL Justifications – CIP-006-6, R1			
			Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR

VRF and VSL Justifications – CIP-006-6, R1			
			The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-006-5 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary in the "Severe" category and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

VRF and VSL Justifications – CIP-006-6, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. This Requirement calls for one or more documented visitor control programs. Failure to implement a visitor control program is not expected to directly affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented visitor control programs. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-5, R2, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-6, R2 is consistent.

VRF and VSL Justifications – CIP-006-6, R2			
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a documented visitor control program is an administrative requirement, and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented visitor control programs and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR

VRF and VSL Justifications – CIP-006-6, R2			
			The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are binary in the “Severe” category and therefore do not lower the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary in the “Severe” category and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

VRF and VSL Justifications – CIP-007-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The Requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports. Depending on the port and the impact classification of the affected cyber asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the Requirement level, and the Requirement Parts are treated equally. Unprotected logical and physical ports are both access points into a BES Cyber System.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R1, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs.

VRF and VSL Justifications – CIP-007-6, R1			
	Failure to disable or prevent access to a single logical or physical port on one BES Cyber System is unlikely to lead to Bulk Electric System instability, separation, or cascading failures. Therefore, this Requirement was assigned a Medium VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Unprotected logical and physical ports are both access points into a BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)

VRF and VSL Justifications – CIP-007-6, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-007-5 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement at the moderate or high VSL category would not necessarily compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R2			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The Requirement requires entities to manage security patches in a proactive way by monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner. Depending on the patch and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-007-5, R2, which has an approved VRF of Medium. Therefore the VRF is consistent with the FERC-approved VRF.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage a security patch on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R2. (R2) OR

VRF and VSL Justifications – CIP-007-6, R2			
evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan	OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

VRF and VSL Justifications – CIP-007-6, R2			
	within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)		

VRF and VSL Justifications – CIP-007-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines— There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but failed to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement a security patch can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability. There may be instances where the security vulnerability is so severe that failure to patch alone can comprise computer network security, but these cases are the exception.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R3			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The requirement requires entities to have processes to limit and detect the introduction of malicious code onto the components of a BES Cyber System. Depending on the malware and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R3, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage malicious code on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR

VRF and VSL Justifications – CIP-007-6, R3			
		The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

VRF and VSL Justifications – CIP-007-6, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R3. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement malicious code protections can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R4			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The requirement requires entities to have processes to provide security event monitoring with the purpose of detecting unauthorized access, reconnaissance, and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. Depending on the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R4, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage security events on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by	The Responsible Entity did not implement or document one or more process(es) that included the

VRF and VSL Justifications – CIP-007-6, R4			
Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (4.4)	applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

VRF and VSL Justifications – CIP-007-6, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R4. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the Requirement.

VRF and VSL Justifications – CIP-007-6, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement Parts for logging required types of events have a binary Severe VSL. Other Requirement Parts associated with security event monitoring do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities establish, implement, and document controls for electronic access to BES Cyber Systems. This includes enforcement of authentication for all user access and CIP Senior Manager, or delegate authorization for use of administrator, shared, default, and other generic account types. It prescribes procedural controls and conditions for changing default passwords and enforcing specific parameters for password based user authentication. Finally, it helps establish a process to limit (where technically feasible) unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for specific actions represented by multiple sub-requirements with a common set of objectives – to ensure the appropriate controls are in place for authorizing and establishing secure electronic access to BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007-5, R5, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement CIP Senior Manager oversight and establish controls to protect BES Cyber Systems from unauthorized electronic access could result in unauthorized access and could directly affect the ability to monitor or control the BES. Although the previous standards versions assigned a VRF of Severe, this is not consistent with the projected risk of BES Cyber System exploitation, which is why the VRF has been modified to Medium.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R5 have a common objective to provide controls to protect against unauthorized electronic access to BES Cyber Systems. The Requirements to authorize and review access, and the

VRF and VSL Justifications – CIP-007-6, R5			
	provided technical and procedural controls to prevent unauthorized access both specify the obligations to provide strong controls to monitor and control electronic access.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

VRF and VSL Justifications – CIP-007-6, R5			
		interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not

VRF and VSL Justifications – CIP-007-6, R5			
			technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

VRF and VSL Justifications – CIP-007-6, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R5. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R5	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations. Gradations are based on the number of unidentified account types, or number of missed controls for authentication and access represent components of the overall requirement that are necessary to fully achieve the reliability of the main requirement.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement parts that can compromise computer network security have a Severe VSL. Other Requirement Parts associated with system access control do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-009-6, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement's VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of implementing and maintaining the recovery plan.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-009-5, R2, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement and maintain the recovery plan is an administrative Requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common objective of implementing and maintaining recovery plans. Requirement Rows 2.1 and 2.3 specify the obligation to implement and test the plan. Requirement Row 2.2 specifies the obligation to maintain backup information used to recover the BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1)

VRF and VSL Justifications – CIP-009-6, R2			
between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

VRF and VSL Justifications – CIP-009-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-009-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-009-6, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this requirement indicates the recovery plan was not properly tested and may have deficiencies, but a violation cannot immediately compromise computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This Requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-010-2, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration change management processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration change management processes can have a medium impact on the reliability and operability of the BES. Although the requirement is administrative in nature and is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration change management. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, R1 specifies the implementation of documented configuration change management processes in conjunction with CIP-010-2, R2, which specifies the implementation of documented configuration monitoring processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R1 requires the implementation of documented configuration change management processes. A failure to implement these documented processes has medium impact on the

VRF and VSL Justifications – CIP-010-2, R1			
	reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-2, Requirement R1 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that

VRF and VSL Justifications – CIP-010-2, R1			
			deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did

VRF and VSL Justifications – CIP-010-2, R1			
			not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

VRF and VSL Justifications – CIP-010-2, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-010-1 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection is not expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R1 specifies that a Responsible Entity must implement and document the processes for configuration change management of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration change management process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-2, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration monitoring processes. A VRF assignment of Medium is consistent with the lower risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration monitoring processes has medium impact on the reliability and operability of the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration monitoring. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, R2 specifies the implementation of documented configuration monitoring processes in conjunction with CIP-010-2, R1, which specifies the implementation of documented configuration change management processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R2 requires the implementation of documented configuration monitoring processes. A failure to implement these documented processes has medium impact on the reliability and operability of the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-010-2, R2			
	CIP-010-1, Requirement R2 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)

VRF and VSL Justifications – CIP-010-2, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines — Severe: the performance measured does not substantively meet the intent of the Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-010-1 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The VSL is binary.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R2 specifies that a Responsible Entity must implement and document the processes for configuration monitoring of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration monitoring process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-011-2, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities prevent unauthorized access to BES Cyber System Information. Failure to adequately identify, protect, and control access to such information could result in unauthorized access and lost, stolen, or misused Cyber System Information. Such failure represents a risk to the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for methods to identify, provide secure handling, and control access to Cyber System Information. The VRF is only applied at the requirement level and the requirement parts are treated equally. The identification, secure handling and control of access have the common objective to protect BES Cyber System Information.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-003, R4 and CIP-003-3, R4.1, which have an approved VRF of Medium. The Requirement also maps to CIP-003-3, R4.2 and CIP-003-3, R4.3 and to CIP-003-3, R5, CIP-003-3, R5.1, CIP-003-3, R5.2, and CIP-003-3, R5.3, which have an approved VRF of Lower. The requirement has the object of securing Cyber System Information. Version 5 combines requirements to ensure consistency. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately identify and protect BES Cyber System Information could result in disclosure of information to unauthorized persons, lost, stolen, or misused Cyber System Information. Such breaches of confidentiality represent a risk to the reliability of Bulk Electric System from misuse by unauthorized persons.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-011-2, R1			
	The sub requirements in R1 have a common objective to assure confidentiality of BES Cyber System Information. The obligations to identify, control access, and assure proper handling of BES Cyber System Information contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

VRF and VSL Justifications – CIP-011-2, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-011-1 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-011-2, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The VSLs are binary for this requirement.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Final Ballots Now Open through November 6, 2014

Now Available

Final ballots for **Critical Infrastructure Protection Standards Version 5 Revisions** are open through **8 p.m. Eastern Thursday, November 6, 2014.**

The final ballots are as follows:

- CIP-003-6 - Cyber Security — Security Management Controls
- CIP-004-6 - Cyber Security — Personnel & Training
- CIP-006-6 - Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-6 - Cyber Security — Systems Security Management
- CIP-009-6 - Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-2 - Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-2 - Cyber Security — Information Protection
- Implementation Plan

Background information for this project can be found on the project page.

Please note that the standards and implementation plan balloted as Version X during the additional ballot are the standards and implementation plan being posted for final ballot. The standards balloted as CIP-003-6 and CIP-010-2 during the additional ballot are undergoing further revisions by the standard drafting team. Therefore, the CIP-003-6 and CIP-010-2 presented for final ballot at this time contain different revisions than the CIP-003-6 and CIP-010-2 presented for additional ballot. NERC added the version numbers to the Version X standards for final ballot in order to prepare them for presentation to the NERC Board of Trustees.

CIP-006-6 and CIP-009-6 are also being posted for final ballot but were not included in the Version X ballot. The votes for CIP-006-6 and CIP-009-6 will be pulled from the initial ballot of those standards. Therefore, you do not have to recast your vote for those standards if your vote remains unchanged from initial ballot.

Instructions for Balloting

In the final ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a vote during the last ballot window may cast a vote in the final ballot window. If a ballot pool member

cast a vote in the previous ballot and does not participate in the final ballot, that member's vote will be carried over in the final ballot.

Members of the ballot pools associated with this project may log in and submit their votes for the standards and implementation plan by clicking here.

Next Steps

The voting results for the standards and implementation plan will be posted and announced after the ballot window closes. If approved, the standards and implementation plan will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities**.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Ryan Stewart, Manager of Standards Development, or Marisa Hecht, Standards Developer, or at 202-644-8091 or 404-446-9620.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions

Final Ballot Results

Now Available

Final ballots for **Critical Infrastructure Protection Standards Version 5 Revisions** and one implementation plan concluded at **8 p.m. Eastern, Thursday, November 6, 2014**.

Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballots.

Ballot	Quorum /Approval
CIP-003-6	87.56% / 83.84%
CIP-004-6	87.32% / 95.34%
CIP-006-6	87.07% / 86.00%
CIP-007-6	87.56% / 95.35%
CIP-009-6	87.56% / 91.17%
CIP-010-2	87.80% / 83.88%
CIP-011-2	87.56% / 95.40%
Implementation Plan	86.59% / 92.76%

Background information for this project can be found on the project page.

Next Steps

The standards will be submitted to the Board of Trustees for adoption.

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact either Marisa Hecht (404-446-9620) or Ryan Stewart (202-644-8091).

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2014-02 CIP-003-6_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	359
Total Ballot Pool:	410
Quorum:	**87.56 % The Quorum has been reached**
Weighted Segment Vote:	83.84 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	82	0.872	12	0.128	0	1	18
2 - Segment 2	9	0.5	4	0.4	1	0.1	0	4	0
3 - Segment 3	93	1	65	0.783	18	0.217	0	1	9
4 - Segment 4	34	1	24	0.857	4	0.143	0	2	4
5 - Segment 5	91	1	60	0.789	16	0.211	0	1	14
6 - Segment 6	54	1	40	0.8	10	0.2	0	1	3
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**6.8**	**287**	**5.701**	**62**	**1.099**	**0**	**10**	**51**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Negative	COMMENT RECEIVED
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	

1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		

1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	SUPPORTS THIRD PARTY COMMENTS
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Abstain	
2	MISO	Marie Knox	Abstain	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Abstain	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Negative	COMMENT RECEIVED
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Negative	COMMENT RECEIVED

3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Negative	COMMENT RECEIVED
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY

				COMMENTS
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Negative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Negative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	

5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Negative	COMMENT RECEIVED
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Negative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Negative	COMMENT RECEIVED
5	Southern Company Generation	William D Shultz	Negative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	SUPPORTS THIRD PARTY COMMENTS
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	

5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Negative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Lincoln Electric System	Eric Ruskamp	Negative	COMMENT RECEIVED
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack	Negative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Affirmative	

7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Ballot Results	
Ballot Name:	Project 2014-02 CIP-004-6_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	358
Total Ballot Pool:	410
Quorum:	**87.32 % The Quorum has been reached**
Weighted Segment Vote:	95.34 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	91	0.968	3	0.032	0	2	17
2 - Segment 2	9	0.9	9	0.9	0	0	0	0	0
3 - Segment 3	93	1	75	0.915	7	0.085	0	3	8
4 - Segment 4	34	1	22	0.88	3	0.12	0	4	5
5 - Segment 5	91	1	73	0.948	4	0.052	0	0	14
6 - Segment 6	54	1	46	0.958	2	0.042	0	1	5
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	7	0.7	0	0	0	0	0
Totals	**410**	**7.1**	**328**	**6.769**	**19**	**0.331**	**0**	**11**	**52**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	

1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	

2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	

3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	

4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
				SUPPORTS

5	Nebraska Public Power District	Don Schmit	Negative	THIRD PARTY COMMENTS
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	

6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-006-6_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	357
Total Ballot Pool:	410
Quorum:	**87.07 % The Quorum has been reached**
Weighted Segment Vote:	86.00 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	82	0.891	10	0.109	0	7	14
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	64	0.821	14	0.179	0	5	10
4 - Segment 4	34	1	21	0.84	4	0.16	0	3	6
5 - Segment 5	91	1	56	0.8	14	0.2	0	7	14
6 - Segment 6	54	1	41	0.854	7	0.146	0	0	6
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	5	0.5	2	0.2	0	0	0
Totals	**410**	**7.1**	**283**	**6.106**	**51**	**0.994**	**0**	**23**	**53**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Lincoln Electric System	Doug Bantam	Affirmative	

1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Negative	COMMENT RECEIVED
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		

1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer		
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Negative	SUPPORTS THIRD PARTY COMMENTS
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Negative	COMMENT RECEIVED
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY

				COMMENTS
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Abstain	
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Negative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Cowlitz County PUD	Rick Syring	Abstain	
4	DTE Electric	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Abstain	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	

5	Empire District Electric Co.	mike I kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	SUPPORTS THIRD PARTY COMMENTS
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Abstain	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Negative	

5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Negative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Negative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	

6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Negative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Ballot Results	
Ballot Name:	Project 2014-02 CIP-007-6_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	359
Total Ballot Pool:	410
Quorum:	**87.56 % The Quorum has been reached**
Weighted Segment Vote:	95.35 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	91	0.968	3	0.032	0	2	17
2 - Segment 2	9	0.9	9	0.9	0	0	0	0	0
3 - Segment 3	93	1	75	0.915	7	0.085	0	3	8
4 - Segment 4	34	1	22	0.88	3	0.12	0	4	5
5 - Segment 5	91	1	74	0.949	4	0.051	0	0	13
6 - Segment 6	54	1	46	0.958	2	0.042	0	1	5
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	7	0.7	0	0	0	0	0
Totals	**410**	**7.1**	**329**	**6.77**	**19**	**0.33**	**0**	**11**	**51**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	

1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	

2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	

3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	

4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
				SUPPORTS

5	Nebraska Public Power District	Don Schmit	Negative	THIRD PARTY COMMENTS
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	

6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Ballot Results	
Ballot Name:	Project 2014-02 CIP-009-6_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	359
Total Ballot Pool:	410
Quorum:	**87.56 % The Quorum has been reached**
Weighted Segment Vote:	91.17 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	85	0.924	7	0.076	0	7	14
2 - Segment 2	9	0.8	8	0.8	0	0	0	0	1
3 - Segment 3	93	1	68	0.85	12	0.15	0	4	9
4 - Segment 4	34	1	21	0.84	4	0.16	0	3	6
5 - Segment 5	91	1	63	0.863	10	0.137	0	5	13
6 - Segment 6	54	1	43	0.896	5	0.104	0	0	6
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.4	4	0.4	0	0	0	0	1
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	7	0.7	0	0	0	0	0
Totals	**410**	**7.1**	**301**	**6.473**	**38**	**0.627**	**0**	**20**	**51**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg		
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted E Hobson		
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Negative	COMMENT RECEIVED
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	

1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Eric Olson	Abstain	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	

1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker		
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	

3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Cowlitz County PUD	Rick Syring	Abstain	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
				SUPPORTS THIRD

4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	PARTY COMMENTS
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	EDP Renewables North America LLC	Heather Bowden	Affirmative	
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	

5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik		
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff	Negative	COMMENT RECEIVED
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Feather Power Project	Kathryn Zancanella	Abstain	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	

6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Negative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	

8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2014-02 CIP-010-2_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	360
Total Ballot Pool:	410
Quorum:	**87.80 % The Quorum has been reached**
Weighted Segment Vote:	83.88 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	84	0.894	10	0.106	0	1	18
2 - Segment 2	9	0.9	6	0.6	3	0.3	0	0	0
3 - Segment 3	93	1	68	0.829	14	0.171	0	2	9
4 - Segment 4	34	1	23	0.852	4	0.148	0	3	4
5 - Segment 5	91	1	66	0.88	9	0.12	0	3	13
6 - Segment 6	54	1	40	0.8	10	0.2	0	1	3
7 - Segment 7	2	0	0	0	0	0	0	1	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**7.1**	**298**	**5.955**	**51**	**1.145**	**0**	**11**	**50**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Black Hills Corp	Wes Wingen	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	

1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		

1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	SUPPORTS THIRD PARTY COMMENTS
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Negative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	COMMENT RECEIVED
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Negative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Negative	COMMENT RECEIVED
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Negative	COMMENT RECEIVED
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	

4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Negative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
				SUPPORTS

5	Kissimmee Utility Authority	Mike Blough	Negative	THIRD PARTY COMMENTS
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Negative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	SUPPORTS THIRD PARTY COMMENTS
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Negative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	

6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro	Negative	COMMENT RECEIVED
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Negative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Negative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack	Negative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Abstain	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	

10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Ballot Results	
Ballot Name:	Project 2014-02 CIP-011-2_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	359
Total Ballot Pool:	410
Quorum:	**87.56 % The Quorum has been reached**
Weighted Segment Vote:	95.40 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	91	0.968	3	0.032	0	2	17
2 - Segment 2	9	0.9	9	0.9	0	0	0	0	0
3 - Segment 3	93	1	75	0.915	7	0.085	0	3	8
4 - Segment 4	34	1	22	0.88	3	0.12	0	4	5
5 - Segment 5	91	1	73	0.948	4	0.052	0	1	13
6 - Segment 6	54	1	46	0.958	2	0.042	0	1	5
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	7	0.7	0	0	0	0	0
Totals	**410**	**7.2**	**329**	**6.869**	**19**	**0.331**	**0**	**11**	**51**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	

1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	

2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Green Cove Springs	Mark Schultz	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	

3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	COMMENT RECEIVED
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	

4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
				SUPPORTS

5	Nebraska Public Power District	Don Schmit	Negative	THIRD PARTY COMMENTS
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	

6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Ballot Results	
Ballot Name:	Project 2014-02 Implementation_Plan_Final_Ballot_October_2014
Ballot Period:	10/28/2014 - 11/6/2014
Ballot Type:	Final
Total # Votes:	355
Total Ballot Pool:	410
Quorum:	**86.59 % The Quorum has been reached**
Weighted Segment Vote:	92.76 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	113	1	81	0.91	8	0.09	0	4	20
2 - Segment 2	9	0.8	7	0.7	1	0.1	0	1	0
3 - Segment 3	93	1	75	0.938	5	0.063	0	4	9
4 - Segment 4	34	1	25	0.962	1	0.038	0	3	5
5 - Segment 5	91	1	68	0.919	6	0.081	0	4	13
6 - Segment 6	54	1	45	0.957	2	0.043	0	2	5
7 - Segment 7	2	0.1	1	0.1	0	0	0	0	1
8 - Segment 8	5	0.3	3	0.3	0	0	0	0	2
9 - Segment 9	2	0.2	2	0.2	0	0	0	0	0

10 - Segment 10	7	0.7	6	0.6	1	0.1	0	0	0
Totals	**410**	**7.1**	**313**	**6.586**	**24**	**0.515**	**0**	**18**	**55**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Brian Cole	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Affirmative	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky		
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Muhammed Ali	Affirmative	
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	faranak sarbaz	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Jo-Anne M Ross	Affirmative	

1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton		
1	Nebraska Public Power District	Jamison Cawley	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White		
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Otter Tail Power Company	Daryl Hanson		
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southern Illinois Power Coop.	William Hutchison		
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tacoma Power	John Merrell	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Eric Olson	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	

1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Wolverine Power Supply Coop., Inc.	Michelle Clements		
1	Xcel Energy, Inc.	Gregory L Pieper	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Leonard Kula	Affirmative	
2	ISO New England, Inc.	Matthew F Goldberg	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	COMMENT RECEIVED
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Corp.	David J Jendras	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	

3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	Jenn Stover	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell		
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Abstain	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	COMMENT RECEIVED
3	Rutherford EMC	Thomas Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	DTE Electric	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider		
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		

4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Southern Minnesota Municipal Power Agency	Richard L Koch	Abstain	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony P Jankowski	Affirmative	
5	AES Corporation	Leo Bernier		
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Negative	COMMENT RECEIVED
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Negative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	EDP Renewables North America LLC	Heather Bowden		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	

5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Nevada Power Co.	Richard Salgo	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Negative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	SUPPORTS THIRD PARTY COMMENTS
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson		
5	Xcel Energy, Inc.	Mark A Castagneri	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	Calpine Energy Services	Agus Bintoro		
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	

6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	New York Power Authority	Shivaz Chopra	Affirmative	
6	New York State Electric & Gas Corp.	Julie S King	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp		
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Affirmative	
6	Tennessee Valley Authority	Marjorie S Parsons	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Abstain	
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Siemens Energy, Inc.	Frank R. McElvain		
8		David L Kiguel	Affirmative	
8		Debra R Warner		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	New York State Public Service Commission	Diane J Barney	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Karin Schweitzer	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Exhibit G

Standard Drafting Team Roster

Project 2014-02 Standard Drafting Team Roster

Name and Title	Company and Address	Contact Info	Bio
Maggy Powell, NERC Compliance Management	Exelon Corporation 100 Constellation Way, Suite 500P Baltimore, MD 21202	Margaret.Powell@constellation.com (410)470-3382	Maggy Powell has more than twenty years of regulatory risk and government affairs experience covering a broad range of industries including energy, environmental markets, healthcare, scientific research, higher education, and international trade. Ms. Powell currently works in the NERC Compliance Management Team at Exelon Corp. and is responsible for corporate-wide engagement on reliability regulatory matters including development of strategic positions on NERC governance and policy; coordination of technical input on proposed Reliability Standards; promotion of cross-enterprise collaboration; and, resolution of conflicts as appropriate. Exelon is a public utility holding company that, through its utility subsidiaries, distributes electricity to approximately 6.6 million customers in Illinois, Pennsylvania, and Maryland. Exelon has a diverse portfolio of electric generation capacity, and it operates the largest nuclear fleet in the United States. Exelon's operations also include power marketing, transmission, and distribution. At present, Ms. Powell is Co-Chair of the NERC Project 2014-02 CIP Standards V5 Revisions Standards Drafting Team.
Philip Huff Director of IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, AR 72119	(501)570-2444 philip.huff@aecc.com	Philip Huff serves as the Director of Security and Compliance at Arkansas Electric Cooperative where Mr. Huff has worked the past 12 years. Mr. Huff has served as vice chair of the CIP Version 5 Standards Drafting Team and co-chair of the Version 5 Revisions Standards Drafting Team. Mr. Huff has degrees in Mathematics and Computer Science from Harding University and a Masters in Computer Security from James Madison University. Mr. Huff is a CISSP and holds Department of Defense certifications in information system security.

Project 2014-02 Standard Drafting Team Roster

Jay Cribb, Generation Cyber Security Program Manager	Southern Company Services, Inc. 241 Ralph McGill Blvd NE Atlanta, GA 30308	(404)506-3854 jscribb@southernco.com	Jay Cribb has 29 years' experience in the utility industry with Southern Co. All of Mr. Cribb tenure has been spent in areas related to information technology, and he has spent the last 12 years in cyber security roles. Mr. Cribb was a member of the Order 706 SDT working to produce versions 2-5 of the CIP standards and has spent 5 of the last 6 years on CIP drafting teams. Mr. Cribb is a past chair of the EEI Security Committee and remains active in NERC CIPC, SERC CIPC, EEI, NAGF, and other industry organizations devoted to protecting critical infrastructure.
David S. Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, GA 30084	(770)270-7815 david.revill@gatrans.com	David Revill is the Manager of Cyber Security Operations for Georgia Transmission Corporation (GTC), an electric transmission cooperative owned by 38 of Georgia's Electric Membership Cooperatives. Mr. Revill is responsible for the physical and cyber security of GTC's infrastructure including compliance with all NERC CIP Standards. Mr. Revill previously was the Group Lead for the Electronic Maintenance lab at GTC which was responsible for the SCADA, Revenue Metering, and Communications at GTC's field assets. Prior to joining GTC, Mr. Revill held positions supporting SCADA/EMS systems for control centers as a SCADA Systems Support Engineer and a Process Controls Network Engineer with Entergy. Mr. Revill is the vice-chair of the North American Transmission Forum Security Practices Group. Mr. Revill is also a member of the NERC Critical Infrastructure Protection Committee (CIPC) Executive Committee representing NRECA, the SERC CIPC, the Electricity Subsector Coordinating Council Senior Executive Working Group, and has been a member of the NERC CIP Standards Drafting Team beginning with version 2 of the CIP Standards.

Project 2014-02 Standard Drafting Team Roster

			Mr. Revill holds a Master's degree in Electrical and Computer Engineering from Georgia Tech and dual bachelor's degrees in Electrical Engineering and Computer Engineering from the Tulane University. Mr. Revill is also currently pursuing an MBA at the University of Florida.
Christine Hasha, CIP Compliance Lead Advisor	Electric Reliability Council of Texas, Inc. 2705 W. Lake Dr. Taylor TX 76574	(512)248-3909 chasha@ercot.com	Christine Hasha brings over 20 years' experience in Information Technology with an emphasis on Information Security and regulatory compliance. Ms. Hasha has a CISSP, and holds a degree in Management from St. Edward's University. Ms. Hasha has extensive experience in development of security policies and controls. Ms. Hasha brings experience and training in common control frameworks including previous experience in implementing security controls for banking, Sarbanes-Oxley, GLBA, and HIPAA consistent with IS027001/27002. Ms. Hasha was a member of Project 2008-06 Standards Drafting Team. Ms. Hasha is actively involved with the ERCOT Region CIP Working Group and participates on CIP-related issues for the ISO/RTO Council Standards Review Committee.
David Dockery, Outside Services, NERC Reliability Compliance	Associated Electric Cooperative, Inc. 2814 S Bothwell Ave. Springfield, MO 65804	(417)885-9286 ddockery@aeci.org	David Dockery has thirty years' experience in SCADA/EMS specification, development, modifications, maintenance, and management, including change-management, and later including NERC CIP compliance. Mr. Dockery spent two years as an Ops Engineer and compliance SME for computer systems and Operations related to BA, TOP, GOP, and TSP functions. Mr. Dockery has two years' experience in AECI Compliance Department, for NERC Standards. Former member: MOD-A Standards Drafting Team, and NERC CIP Interpretation Drafting Team. Active Observer for entire CIP Version 5 development process. Active

Project 2014-02 Standard Drafting Team Roster

			Observer for BES Definition Phase-2 development process.
Scott Saunders, Information Security Officer	Sacramento Municipal Utility District 6201 S Street, MS B251 Sacramento, CA 95817	(916)732-5292 scott.saunders@smud.org	Scott Saunders has over 20 years of experience in various information technology disciplines. Mr. Saunders joined the Sacramento Municipal Utility District, an electric utility company in Sacramento, California, in 2007 as the Information Security Officer. Mr. Saunders provides day-to-day leadership, management, and oversight in the implementation of the Critical Infrastructure Protection cybersecurity standards, cybersecurity risk management practices, operational resiliency, and legislative initiatives. Mr. Saunders has contributed in the development of several public-private partnership cybersecurity guidelines; including the Department of Energy (DOE) Risk Management Process (RMP), Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the implementation of the Presidential Executive Order 13636: Improving Critical Infrastructure Cybersecurity. Mr. Saunders is the Vice Chair of the National Institute of Standards and Technology (NIST) and Smart Grid Interoperability Panel (SGIP) Smart Grid Cybersecurity Committee (SGCC) representing the electricity sub-sector. Mr. Saunders is a regular guest panelist nationally on cybersecurity and its impacts to municipal utilities. Mr. Saunders maintains several industry certifications, including the Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM). Mr. Saunders holds both a Bachelor's and Master's of Science in Information Security Assurance.
Forrest Krigbaum, Grid Operations – Information System Security Manager	Bonneville Power Administration 905 NE 11th Ave. Portland, OR 97232	(360)418-2081 fmkrigbaum@bpa.gov	Forrest Krigbaum has over 26 years of progressively responsible experience working on Information Technology and Cyber Security in the Electric Industry. Mr. Krigbaum currently functions as the Transmission Information Security

Project 2014-02 Standard Drafting Team Roster

			programmatic authority and NERC CIP senior manager delegate, responsible for the development and implementation of operational cyber security strategies, policies, processes, guidelines, and projects to safeguard critical cyber assets that are necessary for reliable and secure operation of the Bulk Electric System (BES). Among his significant previous positions, Mr. Krigbaum served as the Compliance Business Partner for the entire BPA organization, by acting as internal auditor on Critical Infrastructure Protection and 693 standards. Mr. Krigbaum provided expert evaluation of BPA evidence for Reliability Standards to ensure agency compliance. Mr. Krigbaum has also served as a BPA Corporate Cyber Security Professional where he managed security risk assessment and reporting activities.
Steven A. Brain, Program Manager ITRM Compliance	Dominion Resources Services, Inc. 707 East Main Street Richmond, VA 23219	(804)771-3987 steve.brain@dom.com	Steven Brain is a Program Manager with Dominion, one the nation's largest producers and transporters of energy. Mr. Brain currently manages the NERC CIP Compliance Program where he is responsible for Critical Infrastructure Protection cybersecurity policy, compliance, and regulatory programs. Mr. Brain is currently a member of the NERC Project 2014-02 CIP Standards V5 Revisions Standards Drafting Team. Mr. Brain has participated in the SERC ISME program where he served as an industry subject matter expert assisting SERC staff during an onsite compliance audit of a large utility in 2012. Mr. Brain has held numerous management roles supporting Dominion's Cyber Security and Compliance programs. These include the following: • Manager –IT DVP Cyber Security & Compliance where he developed the concept and implemented Dominion Virginia Power's cyber security and compliance program.

Project 2014-02 Standard Drafting Team Roster

			• Manager – IT Process Systems where Mr. Brain was responsible for the IT group supporting the Energy Management System used by Electric Transmission's Systems Operations Center. In this role, Mr. Brain enhanced the existing EMS Cyber Security and Compliance program by implementing controls and self-audit techniques. • Manager – IT Risk Operations, where Mr. Brain managed a team of cyber security professionals responsible for operational support of security activities. Prior to Mr. Brain's management responsibilities he held various analyst roles supporting security, network, and telecommunications infrastructure within Dominion's enterprise. In the focus area of security, Mr. Brain conducted audits and performed penetration testing of critical systems using open source and custom scripted tools. Mr. Brain has been instrumental in developing and implementing numerous network security solutions, processes, and procedures currently in use by Dominion. Mr. Brain has over 29 years' experience working in the Utility industry with a concentration on Telecommunications, Information Technology, Cyber Security, and Compliance.
Greg Goodrich, Principal, Security and Compliance Coordination	New York Independent System Operator 10 Krey Boulevard Rensselaer, New York 12144	(518)356-7591 ggoodrich@nyiso.com	Greg Goodrich is the New York Independent System Operator (NYISO) Principal, Security and Compliance Coordination. Mr. Goodrich has over 29 years of experience working with industrial control systems (ICS), supervisory control systems and data acquisition systems (SCADA), energy management systems (EMS), security, and information technology and software. Currently, Mr. Goodrich chairs the NPCC Task Force on Information Security and Technology and serves as a NERC

Project 2014-02 Standard Drafting Team Roster

			Critical Infrastructure Protection Committee (CIPC) representative. Mr. Goodrich is also a member of the ISO/RTO Council (IRC) Security Working Group, which supports cyber security, physical security, and compliance matters. Most recently, Mr. Goodrich is participating as a member of the NERC Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions Standard Drafting Team. Mr. Goodrich is participating on the Electricity Sub-sector Coordinating Council Senior Executive Work Group, which supports activities following the Executive Order (EO 13636) and Presidential Policy Directive 21 (PPD-21), including the Integrated Task Force and the update to the National Infrastructure Protection Plan. Additionally, Mr. Goodrich coordinated the New York State Cybersecurity Exercise 2014 partnering with Department of Energy engaging electric and gas companies in New York State evaluating Cybersecurity responses with local, State and Federal partners. Mr. Goodrich joined the NYISO in 2001, where he supported and lead aspects of the Standard Market Design II (SMD-II) project and DOE Smart Grid Investment Grant project, managed Enterprise Security, and coordinated NYISO's NERC CIP compliance program. Prior to joining the NYISO, Mr. Goodrich worked for Vermont Electric Power Company for 12 years managing IT and SCADA/EMS groups. Mr. Goodrich holds several industry and security certifications including the Certified Information System Security Profession (CISSP).

Exhibit H

Application of Risk-Based Compliance Mentoring and Enforcement Program Concepts to CIP Version 5

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The Application of Risk-based Compliance Monitoring and Enforcement Program Concepts to CIP Version 5

October 22, 2014

The purpose of this document is to demonstrate how NERC's Compliance Monitoring and Enforcement Program (CMEP) will apply risk-based concepts to the compliance monitoring and enforcement of Critical Infrastructure Protection Reliability Standards Version 5 (CIP Version 5). NERC will not set forth an independent, separate compliance monitoring and enforcement program for CIP Version 5. Rather, this document provides guidance as industry transitions to CIP Version 5. Additional information regarding Reliability Assurance Initiative (RAI) projects and programs for risk-based compliance monitoring and enforcement may be found in the standalone program documents, which are referenced herein and are available on NERC's RAI webpage.[1]

Introduction

CIP Version 5 represents a significant improvement – and change – over the currently-effective CIP Version 3, as it adopts new cyber security controls and extends the scope of systems that are protected by the CIP Reliability Standards. On November 22, 2013, FERC issued a final rule approving CIP Version 5. Under the FERC-approved implementation plan, registered entities will transition from compliance with currently-effective CIP Version 3 to CIP Version 5, thereby bypassing implementation of CIP Version 4.

In drafting CIP Version 5, the standards drafting team recognized the need to shift from the "zero tolerance" compliance and enforcement approach of the past with respect to several CIP requirements. This was for two reasons. First, while registered entities must identify, control, and minimize noncompliance, it is not reasonable to expect that registered entities will be able to prevent all noncompliance because of the breadth and high frequency of the cybersecurity obligations. Second, individual instances of noncompliance with these requirements in particular are less likely to pose a more-than-minimal risk to reliability. The standards drafting team recognized that, under these circumstances, the enforcement process would better promote the goals of reliability by focusing efforts and resources on avoiding noncompliance that poses a greater risk to reliability. Using an "identify, assess, and correct" approach, specific language in 17 CIP Version 5 requirements would have required registered entities to implement processes, plans, or procedures in a manner that would "identify, assess, and correct" instances of noncompliance. This approach would have required registered entities to develop internal controls and would have enabled noncompliance posing a minimal risk to reliability to be addressed outside of the enforcement process.

In Order No. 791, FERC directed NERC to develop modifications to the CIP Version 5 Standards. Among those modifications, FERC directed NERC to modify the "identify, assess, and correct" language in the 17

[1] http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

CIP Version 5 requirements that contained it. While expressing its receptivity to other options, FERC indicated its preference that NERC remove the "identify, assess, and correct" language from the body of the standards, and further indicated its preference not to include compliance language in the standards requirements. In lieu of replacing the "identify, assess, and correct" language, FERC suggested that NERC develop a compliance and enforcement approach, through the CMEP, that would empower NERC and the Regional Entities to exercise risk-based enforcement discretion.

The Way Forward: the Reliability Assurance Initiative

In November 2012, the ERO Enterprise launched a multi-year effort, known as RAI, to identify and implement changes to enhance the effectiveness of the CMEP by using a risk-based approach. A risk-based approach is necessary for a proper allocation of ERO Enterprise resources, enables a process that focuses on improved reliability, and encourages registered entities to enhance internal controls, including those regarding the self-identification of noncompliance.

Further, the ERO Enterprise recognized that it is not practical, effective, or sustainable to monitor and treat all compliance issues to the same degree or in the same manner. Compliance monitoring and enforcement must be "right-sized" based on a number of considerations, including risk factors and registered entity management practices related to the detection, assessment, mitigation, and reporting of noncompliance.

In response to Order No. 791, the ERO determined that it would be useful to explain how the compliance monitoring and enforcement of CIP Version 5 will necessarily be shaped by risk-based CMEP concepts. The risk-based CMEP approach incorporates the fundamental rationale and principles of the self-correcting "identify, assess, and correct" language and applies it to all Reliability Standards. This approach:

- Recognizes that not all noncompliance requires formal enforcement action;
- Recognizes and rewards registered entities for efforts to improve internal controls and methods for the prompt self-identification and mitigation of noncompliance;
- Maintains ERO Enterprise visibility into all noncompliance to identify reliability risks and trends; and
- Maintains NERC oversight to identify implementation issues and opportunities for improvement.

The ERO Enterprise is well on its way to implementing the risk-based CMEP approach. Over the course of 2013-2014, the ERO Enterprise tested a number of concepts, processes, and programs for complete implementation in 2015. The ERO Enterprise is gaining experience – now – applying risk-based enforcement concepts to noncompliance with CIP Reliability Standards. For example, a substantial portion of the compliance exceptions that have been processed as part of the limited rollout of that program have resolved instances of noncompliance with CIP Reliability Standards. Beginning in 2015, the ERO Enterprise will consider all minimal risk noncompliance from all registered entities to be eligible for compliance exception treatment.

The risk-based CMEP concepts are discussed below.

Compliance Monitoring of CIP Version 5

The transformation for compliance monitoring involves the use of the oversight plan framework (Framework).[2] The Framework focuses on identifying, prioritizing, and addressing risks to the bulk power system (BPS), which enable each Regional Entity to allocate resources where they are most needed and likely to be the most effective. The result is a compliance oversight plan for each individual registered entity.

The ERO Enterprise's migration to a risk-based strategy for compliance monitoring includes a significant focus on cybersecurity and the CIP Version 5 Reliability Standards. The inherent risk assessment and internal control evaluation will be essential components for the monitoring of compliance with CIP Version 5.

Inherent Risk Assessment (IRA)

The Regional Entities conduct IRAs for the registered entities within their regions. An IRA is a review of potential risks posed by an individual registered entity to the reliability of the BPS. An IRA considers factors such as assets, systems, geography, interconnectivity, and functions performed, among others. The IRA enables the Regional Entities to tailor oversight appropriately. For example, a Regional Entity may choose not to include in the scope of its monitoring activities certain standards or requirements if the IRA shows less risk to reliability for those standards or requirements for that registered entity. Conversely, a Regional Entity may choose to focus its monitoring on areas for which the IRA shows greater risk.

CIP Version 5 was designed to apply security controls to those systems and processes that could cause the most significant impact to the grid. Therefore, in conducting the IRA for a Responsible Entity under CIP Version 5, the Regional Entity would consider, among other things, the Bulk Electric System (BES) Cyber System Categorization analysis developed pursuant to CIP-002-5.1 R1. This standard provides "bright-line" criteria for registered entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect reliable BES operation.

By understanding the entity's high, medium, and low impact BES Cyber Systems, the Regional Entities are able to tailor the compliance monitoring to the entity's risk and identify which systems in each category should be the focus of compliance monitoring activities.

Internal Control Evaluation (ICE)

Following the IRA, a registered entity may elect to provide information concerning the internal controls it uses to manage reliability risks to help focus the compliance oversight efforts of the Regional Entity. The process by which this evaluation takes place is called the ICE. The ICE is a voluntary process, and registered entities are not obligated to participate. However, the evaluation of internal controls may be

[2] *See, e.g.*, Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program (Sep. 5, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Overview%20of%20the%20ERO%20Enterprise's%20Risk-Based%20CMEP.pdf. *See also* 2015 ERO Compliance Monitoring and Enforcement Implementation Plan (Sep. 8, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_2015%20CMEP%20IP_V7_090814.pdf.

especially useful for tailoring compliance monitoring activities in the CIP context, as CIP Version 5 requires system or device level controls on hundreds of facilities that may operate thousands of devices.

As described in the ERO Enterprise Internal Control Evaluation Guide (ICE Guide),[3] the ICE may inform whether a registered entity has implemented effective internal controls that provide reasonable assurance of compliance with Reliability Standards associated with areas of risk identified through the IRA. The Regional Entity uses the IRA to identify the risks applicable to the registered entity and uses the ICE to understand how the registered entity manages or mitigates those risks to further tailor monitoring activities. The ICE is designed to be scalable, recognizing that the make-up of an internal control program will vary in accordance with the registered entity's size and complexity.

Monitoring Tools

Ultimately, the Regional Entity will determine the type and frequency of the compliance monitoring tools (i.e., off-site or on-site audits, spot checks, or self-certifications) warranted for a particular registered entity based on reliability risks, as determined through the IRA and, if applicable, ICE processes. The Regional Entity may conduct more resource-intensive compliance monitoring activities with respect to functions or registered entities within its region that can have the most significant impact on reliability of the BPS, as determined through the IRA. For functional roles or registered entities that have a lesser impact on reliability to the BPS, the Regional Entity may tailor compliance monitoring approaches accordingly.

Example of Risk-Based Compliance Monitoring Approach to CIP Version 5

This example will refer to hypothetical entity called "ABC Co."

The Regional Entity performs an IRA for ABC Co., which is located within its region. As determined through the CIP-002-5.1 analysis, ABC Co. has numerous high and medium impact BES Cyber Systems. The Regional Entity considers ABC Co.'s geography, interconnectivity, and functions performed. From this assessment, the Regional Entity determines that workforce capability issues at ABC Co. could pose greater risk to reliability.

Therefore, as a result of its IRA, the Regional Entity proposes to include Reliability Standards that address the security of networks, Supervisory Control and Data Acquisition/Energy Management Systems (SCADA/EMS), and the personnel that support them. As part of its compliance oversight plan for ABC Co., the Regional Entity determines to place special emphasis on the following Reliability Standards for its next Compliance Audit of ABC Co.: CIP-002, CIP-004, CIP-005, and CIP-007.

ABC Co. is confident that its internal controls relating to its networks, SCADA/EMS, and personnel are well-designed and effective. ABC Co. agrees to participate in an ICE. As part of this ICE, ABC Co. provides documentation regarding the following to the Regional Entity:

- Management philosophy and communication in support of its internal compliance program;
- Evidence of yearly compliance assessments performed by independent firms; and

[3] The ERO Enterprise Internal Control Evaluation Guide (Oct. 2014) (ICE Guide), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Internal%20Control%20Evaluation%20Guide.pdf.

- Internal Audit Division with department goals and measures to ensure compliance with Reliability Standards.

The Regional Entity follows the process set forth in the ICE Guide to identify which of the internal controls provided by ABC Co. are considered "key" in support of the Reliability Standards in scope as part of the compliance oversight plan and should be tested. For example, the Regional Entity may review the following information and validating measures relating to internal controls for CIP-005 R1:[4]

- Electronic Security Perimeter diagrams indicating access points to applicable systems connected to a network via a routable protocol;
- Electronic Access Point network configurations, access lists, or firewall rules;
- The results of annual vulnerability assessments to identify points of access to BES Cyber Systems.

The Regional Entity then begins the process of evaluating the selected key controls in accordance with the methods set forth in the ICE Guide. With the key controls selected for testing, the Regional Entity has the information available to make decisions about the effectiveness of ABC Co.'s internal controls for the in-scope standards and more importantly, the effectiveness of the overall internal control program and whether it provides reasonable assurance of compliance.

In light of the information obtained through the IRA and ICE processes, the Regional Entity decides to define the following compliance monitoring plan for ABC Co.:

- Tri-annual Compliance Audit: ABC Co.'s tri-annual audit would be based primarily on the Reliability Standards identified by the IRA (CIP-002, CIP-004, CIP-005, and CIP-007), with limited reviews and testing of other Reliability Standards. Depending on the results of the ICE, the Regional Entity may adjust the amount of testing to be performed during the audit.
- Guided Self-Certifications: ABC Co. would demonstrate compliance with other applicable Reliability Standards by providing compliance information or evidence of controls through a Self-Certification program customized to ABC Co.'s IRA and ICE results.
- Regular Tests of Key Controls: The Regional Entity would assess any changes to ABC Co.'s internal control program to ensure overall program effectiveness.

Enforcement of Noncompliance for CIP Version 5

Over the past several years, the ERO Enterprise has been migrating to a risk-based strategy of assessing and processing noncompliance. Initially, each instance of noncompliance with the CIP Reliability Standards became a Possible Violation filed in a Notice of Penalty. By introducing the Find, Fix, Track and Report (FFT) process in 2011, the ERO Enterprise recognized that not all violations required the imposition of monetary penalties. The FFT process has successfully resolved over 2,000 instances of noncompliance with the Reliability Standards outside of a Notice of Penalty. Most of these FFTs posed a minimal risk to the reliability of the BPS, and 55% of them involved noncompliance with CIP Reliability Standards.

[4] The list of controls and measures provided here is for illustrative purposes only and should not be interpreted as an exhaustive or complete list of possible controls or an indication of which key controls a Regional Entity may choose to test or find acceptable in a specific case. Registered entities should consult the ICE Guide for further information regarding the ICE process.

Building on its experience with a streamlined process and a reduced record, the ERO Enterprise is implementing two major programs that were developed under RAI to continue the shift toward a risk-based model of enforcement. These programs mark the continued migration away from a "zero tolerance" approach, where all instances of noncompliance are evaluated as Possible Violations. These programs leverage existing internal practices at registered entities relating to self-monitoring, identification, assessment, and correction of noncompliance with Reliability Standards. By appropriately valuing and rewarding such efforts (i.e., by providing a disposition path outside of a formal enforcement action), the ERO Enterprise encourages the enhancement of internal controls and self-identification of noncompliance throughout the industry. These programs include the expansion of risk-based enforcement discretion (compliance exceptions) and the self-logging program.

These risk-based programs embody many of the same risk-based concepts of the "identify, assess, and correct" approach. However, these approaches apply to all Reliability Standards and requirements, not just the 17 CIP Version 5 requirements containing the "identify, assess, and correct" language.

Compliance Exceptions

Since 2013, the ERO Enterprise has exercised discretion when deciding whether to initiate an enforcement action for noncompliance posing a minimal risk to the reliability of the BPS. Issues resolved outside of an enforcement action are referred to as **compliance exceptions.**

Compliance exceptions reflect the "identify, assess, and correct" tenet that not all noncompliance requires processing in a formal enforcement action. Compliance exception treatment is especially appropriate if the registered entity adequately identifies its noncompliance, assesses the risk properly as minimal risk, and corrects (i.e. mitigates) the noncompliance in a timely and appropriate manner. A robust internal compliance program and management practices that led to timely discovery and timely mitigation of noncompliance would create a strong argument in favor of compliance exception treatment. However, all minimal risk noncompliance is eligible regardless of discovery method.

Compliance exceptions are similar to FFT remediated issues in that they will not incur any financial penalty. However, compliance exceptions differ from FFT remediated issues in several important ways. First, compliance exceptions are not subject to formal enforcement processes. Further, a compliance exception is part of a registered entity's compliance history only to the extent that it serves to inform the ERO Enterprise of potential risk. Compliance exceptions are not part of a registered entity's violation history for purposes of aggravation of penalties. Finally, to maintain visibility and allow for appropriate oversight, all compliance exceptions will be documented, submitted to NERC for review, and reported to FERC.

Beginning in 2015, all minimal risk noncompliance from all registered entities will be eligible for compliance exception treatment. Additional information about compliance exceptions is available in the Compliance Exception Overview document.[5]

The ERO Enterprise is gaining experience identifying appropriate CIP noncompliance for compliance exception treatment. A substantial portion of the compliance exceptions processed during the limited

[5] Compliance Exception Overview (Oct. 1, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf.

rollout of the program in 2013-2014 have resolved instances of noncompliance with CIP Reliability Standards.

Self-Logging Program

The self-logging program allows select registered entities with demonstrated effective management practices to self-monitor and identify, assess, and correct (i.e., mitigate) instances of noncompliance to log minimal risk noncompliance that would otherwise be individually self-reported. The Regional Entity confirms, following a periodic submission of the registered entity's log, that the registered entity has adequately identified and described the noncompliance, accurately assessed the risk, and appropriately mitigated the noncompliance. Once the review process is complete, the minimal risk issue is resolved as a compliance exception absent additional risk factors or other issues. This is consistent with the notion that noncompliance that is self-identified through internal controls, corrected through a strong compliance culture, and documented by the registered entity, should not be resolved through the enforcement process or incur a penalty, absent a higher risk to the BPS.

The experience of the ERO Enterprise to date has shown that logs increase visibility into noncompliance detected and corrected at the registered entity, as registered entities are more likely to record instances of noncompliance on their logs than self-report them. Further, the program fosters efficiency and reduces certain formal administrative processes associated with individual Self-Reports.

Participation in the self-logging program is voluntary. Also, the program is not limited to those CIP Version 5 Reliability Standards that originally contained the "identify, assess, and correct" language.

Additional information about the self-logging program, including eligibility, program operation, and the benefits of the program, is available in the Self-Logging of Minimal Risk Issues Program Overview.[6]

Example of Possible Risk-Based Enforcement Approach to CIP Version 5 Noncompliance

For this example, the ABC Co., which is described in the compliance monitoring portion of this document, is again referenced.

ABC Co. discovers that an employee completed CIP cybersecurity training 15 months and two weeks after the date the employee previously completed the training (CIP-004-5.1 R2). ABC Co. has identified this issue as posing a minimal risk to the reliability of the BPS.

If ABC Co. is allowed to self-log this noncompliance, it will log the noncompliance and actions taken to mitigate the noncompliance and prevent recurrence. Following review by the Regional Entity, there is a presumption that the noncompliance will be treated as a compliance exception unless the noncompliance is ineligible for such treatment (e.g., the noncompliance posed a greater than minimal risk, was the result of intentional or willful acts or omissions, or was the result of systemic or significant performance failures).

[6] Self-Logging of Minimal Risk Issues Program Overview (Oct. 1, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Self-logging%20of%20Minimal%20Risk%20Issues%20Program%20Overview.pdf.

If ABC Co. is not allowed to self-log this noncompliance, it may be considered for compliance exception treatment (although there is no presumption). In that case, ABC Co. is encouraged to submit a Self-Report to its Regional Entity.

If the Regional Entity discovered the noncompliance during a Compliance Audit, instead of ABC Co. discovering it on its own, the noncompliance would still be eligible for compliance exception treatment. Whether the minimal risk noncompliance will actually be afforded compliance exception treatment will be determined through a review of the facts and circumstances.

A Regional Entity may determine that compliance exception treatment is not appropriate, for example, when the following facts and circumstances are present:

- Employees have found a way to circumvent the internal controls ABC Co. has in place to ensure the timely completion of training;
- As a result of major turnover in ABC Co.'s compliance department, there is no longer any effective control, practice, or system to ensure training is completed in a timely manner;
- Employees are generally not aware of CIP obligations;
- Multiple employees at ABC Co. are completing training late (or not at all);
- ABC Co. did not discover the issue promptly;
- ABC Co. did not mitigate the issue promptly;
- The underlying issue was foreseeable and could easily happen again (poor internal controls).

In considering whether to afford compliance exception treatment, the Regional Entity may consider, for example, the following facts and circumstances as those weighing in favor of compliance exception treatment:

- ABC Co. had internal controls in place to ensure timely completion of training, including issuing automated training reminder emails and disabling network access when training is not completed on time. However, the employee was on an extended leave, so he did not see the emails or notice when his network access was disabled;
- ABC Co. self-identified the issue through regular reviews of its records;
- ABC Co. has a limited number of employees completing training late;
- ABC Co. experienced an unforeseeable technical issue;
- ABC Co. addressed the issue with its employee promptly;
- The employee completed CIP training in previous years;
- ABC Co. employees are generally aware of CIP obligations.

To summarize, if ABC Co. is allowed to self-log this noncompliance, there is a presumption that the noncompliance will be afforded compliance exception treatment. If ABC Co. is not allowed to self-log this noncompliance, there is no presumption of compliance exception treatment. However, the

noncompliance is still eligible for compliance exception treatment regardless of how it was discovered (e.g., Self-Report, Compliance Audit).

Exhibit I

Mapping Document

Project 2014-02 - CIP Version 5 Revisions

Mapping Document Showing Translation of the Version 5 standards into CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 (CIP-002-5.1, CIP-005-5, and CIP-008-5 were not modified)

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R1	CIP-003-6 R1	To incorporate a policy or policies for low impact BES Cyber Systems, the main requirement language was modified. "For its high impact and medium impact BES Cyber Systems" was struck from the language as new requirement parts were created. See below for part 1.1 and part 1.2 to see the change justification.
NEW	CIP-003-6 R1.1	"For its high impact and medium impact BES Cyber Systems" was added as a qualifier to the sub-parts below.
CIP-003-5 R1.1	CIP-003-6 R1.1.1	Requirement parts for 1.1 through 1.9 have become 1.1.1 through 1.1.9 with the clarifier added above in part 1.1 of CIP-003-6.
CIP-003-5 R1.2	CIP-003-6 R1.1.2	No change.
CIP-003-5 R1.3	CIP-003-6 R1.1.3	No change.
CIP-003-5 R1.4	CIP-003-6 R1.1.4	No change.
CIP-003-5 R1.5	CIP-003-6 R1.1.5	No change.
CIP-003-5 R1.6	CIP-003-6 R1.1.6	No change.
CIP-003-5 R1.7	CIP-003-6 R1.1.7	No change.
CIP-003-5 R1.8	CIP-003-6 R1.1.8	No change.
CIP-003-5 R1.9	CIP-003-6 R1.1.9	No change.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-003-6 R1.2	"For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:" was added as a qualifier to the sub-parts below.
CIP-003-5 R2	CIP-003-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. Furthermore, as the SDT modified its approach of using Attachment 1 instead of the table approach, it modified Requirement R2 to "implement one or more document cyber security plan(s) that include the applicable elements in Attachment 1."
CIP-003-5 R2.1	CIP-003-6 R1.2.1	The security awareness requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.1.
CIP-003-5 R2.2	CIP-003-6 R1.2.2	The physical security controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.2.

Standard: CIP-003-5 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-5 R2.3	CIP-003-6 R1.2.3	The electronic access controls requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.3. Furthermore, the SDT modified the "external routable protocol connections" as a new definition is being proposed by the SDT for "Low Impact External Routable Connectivity."
CIP-003-5 R2.4	CIP-003-6 R1.2.4	The incident response to a Cyber Security Incident requirement part for inclusion in one or more of the documented cyber security policies was moved to CIP-003-6, Requirement R1, Part 1.2.4.
NEW	CIP-003-6, Attachment 1	CIP-003-6 Attachment 1 lists the elements required for low impact asset cyber security plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the lack of objective criteria for Low Impact assets protections.
CIP-003-5 R3	CIP-003-6 R3	No change.
CIP-003-5 R4	CIP-003-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R1	CIP-004-6 R1	No change.
CIP-004-5.1 R1.1	CIP-004-6 R1.1	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2	CIP-004-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase "in a manner that identifies, assesses, and corrects deficiencies" was stricken. The SDT has also revised the requirement to allow Responsible Entities the flexibility to have one or more cyber security training programs, as the existing CIP-004-5 R2 had Responsible Entities shall implement "a cyber security training program(s)." That modification was made for clarity and consistency across the standards.
CIP-004-5.1 R2.1	CIP-004-6 R2.1	No change.
CIP-004-5.1 R2.1.1	CIP-004-6 R2.1.1	No change.
CIP-004-5.1 R2.1.2	CIP-004-6 R2.1.2	No change.
CIP-004-5.1 R2.1.3	CIP-004-6 R2.1.3	No change.
CIP-004-5.1 R2.1.4	CIP-004-6 R2.1.4	No change.
CIP-004-5.1 R2.1.5	CIP-004-6 R2.1.5	No change.
CIP-004-5.1 R2.1.6	CIP-004-6 R2.1.6	No change.
CIP-004-5.1 R2.1.7	CIP-004-6 R2.1.7	No change.
CIP-004-5.1 R2.1.8	CIP-004-6 R2.1.8	No change.
CIP-004-5.1 R2.1.9	CIP-004-6 R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Registered Entity's cyber security training program. The training must address cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with Transient Cyber Assets and Removable Media.
CIP-004-5.1 R2.2	CIP-004-6 R2.2	No change.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R2.3	CIP-004-6 R2.3	No change.
CIP-004-5.1 R3	CIP-004-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R3.1	CIP-004-6 R3.1	No change.
CIP-004-5.1 R3.2	CIP-004-6 R3.2	No change.
CIP-004-5.1 R3.2.1	CIP-004-6 R3.2.1	No change.
CIP-004-5.1 R3.2.2	CIP-004-6 R3.2.2	No change.
CIP-004-5.1 R3.3	CIP-004-6 R3.3	No change.
CIP-004-5.1 R3.4	CIP-004-6 R3.4	No change.
CIP-004-5.1 R3.5	CIP-004-6 R3.5	No change.
CIP-004-5.1 R4	CIP-004-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-004-5.1 R4.1	CIP-004-6 R4.1	No change.
CIP-004-5.1 R4.1.1	CIP-004-6 R4.1.1	No change.
CIP-004-5.1 R4.1.2	CIP-004-6 R4.1.2	No change.
CIP-004-5.1 R4.1.3	CIP-004-6 R4.1.3	No change.
CIP-004-5.1 R4.2	CIP-004-6 R4.2	No change.
CIP-004-5.1 R4.3	CIP-004-6 R4.3	No change.
CIP-004-5.1 R4.4	CIP-004-6 R4.4	No change.
CIP-004-5.1 R5	CIP-004-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.

Standard: CIP-004-5.1– Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-5.1 R5.1	CIP-004-6 R5.1	No change.
CIP-004-5.1 R5.2	CIP-004-6 R5.2	No change.
CIP-004-5.1 R5.3	CIP-004-6 R5.3	No change.
CIP-004-5.1 R5.4	CIP-004-6 R5.4	No change.
CIP-004-5.1 R5.5	CIP-004-6 R5.5	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-5 R1	CIP-006-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R1.1	CIP-006-6 R1.1	No change.
CIP-006-5 R1.2	CIP-006-6 R1.2	No change.
CIP-006-5 R1.3	CIP-006-6 R1.3	No change.
CIP-006-5 R1.4	CIP-006-6 R1.4	No change.
CIP-006-5 R1.5	CIP-006-6 R1.5	No change.
CIP-006-5 R1.6	CIP-006-6 R1.6	No change.
CIP-006-5 R1.7	CIP-006-6 R1.7	No change.
CIP-006-5 R1.8	CIP-006-6 R1.8	No change.
CIP-006-5 R1.9	CIP-006-6 R1.9	No change.

Standard: CIP-006-5 – Cyber Security—Physical Security of BES Cyber Systems		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-006-6 R1.10	To respond to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. There are three other mechanisms for an entity to adequately protect those networks, including encryption of data that transits such cabling and components; monitoring the status of the communication link and issuing alarms to detect communication failures; or an equally effective logical protection.
CIP-006-5 R2	CIP-006-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-006-5 R2.1	CIP-006-6 R2.1	No change.
CIP-006-5 R2.2	CIP-006-6 R2.2	No change.
CIP-006-5 R2.3	CIP-006-6 R2.3	No change.
CIP-006-5 R3	CIP-006-6 R3	No change.
CIP-006-5 R3.1	CIP-006-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R1	CIP-007-6 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R1.1	CIP-007-6 R1.1	No change.
CIP-007-5 R1.2	CIP-007-6 R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions address the communication networks directive from FERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
CIP-007-5 R2	CIP-007-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R2.1	CIP-007-6 R2.1	No change.
CIP-007-5 R2.2	CIP-007-6 R2.2	No change.
CIP-007-5 R2.3	CIP-007-6 R2.3	No change.
CIP-007-5 R2.4	CIP-007-6 R2.4	No change.
CIP-007-5 R3	CIP-007-6 R3	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R3.1	CIP-007-6 R3.1	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R3.2	CIP-007-6 R3.2	No change.
CIP-007-5 R3.3	CIP-007-6 R3.3	No change.
CIP-007-5 R4	CIP-007-6 R4	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R4.1	CIP-007-6 R4.1	No change.
CIP-007-5 R4.1.1	CIP-007-6 R4.1.1	No change.
CIP-007-5 R4.1.2	CIP-007-6 R4.1.2	No change.
CIP-007-5 R4.1.3	CIP-007-6 R4.1.3	No change.
CIP-007-5 R4.2	CIP-007-6 R4.2	No change.
CIP-007-5 R4.2.1	CIP-007-6 R4.2.1	No change.
CIP-007-5 R4.2.2	CIP-007-6 R4.2.2	No change.
CIP-007-5 R4.3	CIP-007-6 R4.3	No change.
CIP-007-5 R4.4	CIP-007-6 R4.4	No change.
CIP-007-5 R5	CIP-007-6 R5	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.
CIP-007-5 R4	CIP-007-6 R4	No change.
CIP-007-5 R5	CIP-007-6 R5	No change.
CIP-007-5 R5.1	CIP-007-6 R5.1	No change.
CIP-007-5 R5.2	CIP-007-6 R5.2	No change.
CIP-007-5 R5.3	CIP-007-6 R5.3	No change.

Standard: CIP-007-5 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-5 R5.4	CIP-007-6 R5.4	No change.
CIP-007-5 R5.5	CIP-007-6 R5.5	No change.
CIP-007-5 R5.5.1	CIP-007-6 R5.5.1	No change.
CIP-007-5 R5.5.2	CIP-007-6 R5.5.2	No change.
CIP-007-5 R6	CIP-007-6 R6	No change.
CIP-007-5 R7	CIP-007-6 R7	No change.

Standard: CIP-009-5 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-5 R1	CIP-009-6 R1	No change.
CIP-009-5 R1.1	CIP-009-6 R1.1	No change.
CIP-009-5 R1.2	CIP-009-6 R1.2	No change.
CIP-009-5 R1.3	CIP-009-6 R1.3	No change.
CIP-009-5 R1.4	CIP-009-6 R1.4	No change.
CIP-009-5 R1.5	CIP-009-6 R1.5	No change.
CIP-009-5 R2	CIP-009-6 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-009-5 R2.1	CIP-009-6 R2.1	No change.
CIP-009-5 R2.2	CIP-009-6 R2.2	No change.
CIP-009-5 R2.3	CIP-009-6 R2.3	No change.
CIP-009-5 R3	CIP-009-6 R3	No change.
CIP-009-5 R3.1	CIP-009-6 R3.1	No change.
CIP-009-5 R3.1.1	CIP-009-6 R3.1.1	No change.
CIP-009-5 R3.1.2	CIP-009-6 R3.1.2	No change.
CIP-009-5 R3.1.3	CIP-009-6 R3.1.3	No change.
CIP-009-5 R3.2	CIP-009-6 R3.2	No change.
CIP-009-5 R3.2.1	CIP-009-6 R3.2.1	No change.
CIP-009-5 R3.2.2	CIP-009-6 R3.2.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R1	CIP-010-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R1.1	CIP-010-2 R1.1	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.2	CIP-010-2 R1.2	No change.
CIP-010-1 R1.3	CIP-010-2 R1.3	No change.
CIP-010-1 R1.4	CIP-010-2 R1.4	No change.
CIP-010-1 R1.4.1	CIP-010-2 R1.4.1	No change.
CIP-010-1 R1.4.2	CIP-010-2 R1.4.2	No change.
CIP-010-1 R1.4.3	CIP-010-2 R1.4.3	No change.
CIP-010-1 R1.5	CIP-010-2 R1.5	No change.
CIP-010-1 R1.5.1	CIP-010-2 R1.5.1	No change.
CIP-010-1 R1.5.2	CIP-010-2 R1.5.2	No change.
CIP-010-1 R2	CIP-010-2 R2	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-010-1 R2.1	CIP-010-2 R2.1	No change.
CIP-010-1 R3	CIP-010-2 R3	No change.
CIP-010-1 R3.1	CIP-010-2 R3.1	No change.
CIP-010-1 R3.2	CIP-010-2 R3.2	No change.

Standard: CIP-010-1 – Cyber Security—Configuration Change Management and Vulnerability Assessments		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-010-1 R3.2.1	CIP-010-2 R3.2.1	No change.
CIP-010-1 R3.2.2	CIP-010-2 R3.2.2	No change.
CIP-010-1 R3.3	CIP-010-2 R3.3	No change.
CIP-010-1 R3.4	CIP-010-2 R3.4	No change.
NEW	CIP-010-2 R4	To respond to the FERC Order No. 791 directive to address transient devices, the SDT modified its approach to use Attachment 1 instead of the table approach. It modified Requirement R4 to "implement one or more documented plan(s) for Transient Cyber Asset and Removable Media that include the applicable elements in Attachment 1, except under CIP Exceptional Circumstances."
NEW	CIP-010-2, Attachment 1	CIP-010-2 Attachment 1 lists the elements required for Transient Cyber Asset and Removable Media Plan(s). The attachment satisfies the directive from FERC Order No. 791 on addressing the risks posed by transient devices.

Standard: CIP-011-1 – Cyber Security—Information Protection		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-1 R1	CIP-011-2 R1	To respond to the FERC Order No. 791 directive to remove ambiguous language from the requirement, the phrase “in a manner that identifies, assesses, and corrects deficiencies” was stricken.
CIP-011-1 R1.1	CIP-011-2 R1.1	No change.
CIP-011-1 R1.2	CIP-011-2 R1.2	No change.
CIP-011-1 R2	CIP-011-2 R2	No change.
CIP-011-1 R2.1	CIP-011-2 R2.1	No change.
CIP-011-1 R2.2	CIP-011-2 R2.2	No change.