NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 15, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Revisions to the Violation Risk Factors and Violation Severity Levels Assigned to Certain
          Critical Infrastructure Protection Reliability Standards
          Docket No. RM13-5-000

Dear Secretary Bose:

In accordance with Order No. 791,[1] the North American Electric Reliability Corporation ("NERC")
submits proposed revisions to certain Violation Risk Factors ("VRFs") and Violations Severity Levels
("VSLs") assigned to certain Critical Infrastructure Protection ("CIP") Reliability Standards for Federal
Energy Regulatory Commission ("FERC" or "Commission") approval. Specifically, NERC proposes
revisions to the VRFs assigned to:

- CIP-006-5, Requirement R3
- CIP-004-5.1, Requirement R4

NERC is also proposing revisions to the VSLs assigned to:

- CIP-003-5, Requirements R1 and R2
- CIP-004-5.1, Requirement R4
- CIP-008-5, Requirement R2
- CIP-009-5, Requirement R3

The proposed VRF and VSL revisions, provided in Attachment A hereto, are consistent with the
Commission's directives in Order No. 791. NERC respectfully requests that the Commission approve the
proposed VRF and VSL revisions as just, reasonable, not unduly discriminatory or preferential, and in the
public interest.

---

[1]   *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013).

RELIABILITY | ACCOUNTABILITY

I.   Background

In Order No. 791, FERC approved new and modified CIP Reliability Standards, referred to as the CIP version 5 Reliability Standards. Among other things, FERC directed NERC to file revisions to certain VRFs and VSLs assigned to certain CIP Reliability Standards.[2] In particular, FERC directed NERC to modify the VRF assignments for Reliability Standards CIP-006-5, Requirement R3 and CIP-004-5, Requirement R4 from Lower to Medium.[3] Additionally, the Commission directed "modification to the VSLs for certain CIP Reliability Standards to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements."[4]

The Commission directed NERC to file the VRF revisions within 90 days of the effective date of Order No. 791.[5] The Commission did not set a timeframe for filing the VSL modifications. On March 19, 2014, the Commission granted NERC an extension of time until May 15, 2014 to file the VRF modifications.[6] The NERC Board of Trustees approved the proposed VRF and VSL revisions on May 7, 2014.

II.   Notices and Communications

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

Holly A. Hawkins
Assistant General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G St., NW, Suite 600
Washington, DC 20005
202-400-3000
holly.hawkins@nerc.net
shamai.elstein@nerc.net

III.   Proposed VRF and VSL Revisions

Consistent with the Commission's directives in Order No. 791, NERC is proposing to modify (i) the VRFs for CIP-006-5, Requirement R3 and CIP-004-5.1, Requirement R4; and (ii) the VSLs for CIP-003-5,

---

[2]   Order No. 791 at PP 181-84, 192-196, 205-210.

[3]   *Id*. at PP 181-84, 192-196.

[4]   *Id*. at P 205-210.

[5]   *Id*. at PP 184, 196.

[6]   *Notice of Extension of Time*, Docket No. RM13-5-000 (March 19, 2014).

Requirements R1 and R2; CIP-004-5.1, Requirement R4; CIP-008-5, Requirement R2; and CIP-009-5, Requirement R3. The following is a discussion of each of the proposed VRF and VSL Revisions.

With respect to the directive to modify the VSLs associated with the requirements that include the "identify, assess, and correct" language, NERC will submit such modifications when it modifies those requirements consistent with FERC's directive from Order No. 791 to remove or modify that language. There is a NERC standards development project, Project 2014-02 CIP Version 5 Revisions, underway to address the Commission directives from Order No. 791.

a. VSL for CIP-003-5, Requirements R1, R2 and R4

Reliability Standard CIP-003-5 addresses security management controls for cyber security. Requirement R1 of that standard governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. Consistent with the Commission directive,[7] proposes to revise the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language.

The Commission also directed NERC to clarify that the VSLs assigned to Requirement R4 of CIP-003-5 include timeline gradations as set forth in the VSL contained in Exhibit A to the petition for approval of the CIP version 5 Reliability Standards.[8] NERC hereby clarifies that VSLs for CIP-003-5, Requirement R4 include the timeline gradations reflected in Exhibit A to the CIP version 5 petition and as reflected in Attachment A hereto.

b. VRF and VSL for CIP-004-5.1, Requirement R4

Reliability Standard CIP-004-5.1 addresses cyber security personnel and training requirements, and Requirement R4 of that standard obligates a responsible entity to have a process for authorizing access to BES Cyber System Information, including periodic verification that users and accounts are authorized and necessary. Consistent with the Commission's directive,[9] NERC proposes to revise the VRF for CIP-004-5.1, Requirement R4 from a "Lower" designation to a "Medium" designation. Additionally, NERC proposes to revise the VSL assignment for CIP-004-5.1, Requirement R4 to a percentage-based gradation consistent with the Commission's directive.[10]

c. VRF for CIP-006-5, Requirement R3

Reliability Standard CIP-006-5 addresses physical security of BES Cyber Systems, and Requirement R3 of that standard governs implementation of Physical Access Control System maintenance

---

[7]   Order No. 791 at P 206.

[8]   *Id.* at P 207.

[9]   *Id.* at PP 192-196.

[10]   *Id.* at P 208.

and testing programs. Consistent with the Commission's directive,[11] NERC proposes to revise the VRF for CIP-006-5, Requirement R3 from a "Lower" designation to a "Medium" designation.

   d. <u>VSL for CIP-008-5, Requirement R2</u>

  Reliability Standard CIP-008-5 addresses incident reporting and response planning for cyber security. Requirement R2 of that standard governs implementation of documented Cyber Security Incident response plans. Consistent with the Commission's directive,[12] NERC proposed to revise the severe VSL to reduce a gap in months between the high VSL and severe VSL.

   e. <u>CIP-009-5, Requirement R3</u>

  Reliability Standard CIP-009-5 addresses recovery plans for BES Cyber Systems. Requirement R3 of that standard governs maintenance of the recovery plans. Consistent with the Commission's directive,[13] NERC proposed to revise the timeframes contained in the VSLs from 90-210 days to 90-120 days, where appropriate.

IV. Conclusion

  For the foregoing reasons, NERC respectfully requests that the Commission approve the proposed VRF and VSL revisions as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

       Respectfully submitted,

       /S. Shamai Elstein

       Holly A. Hawkins
       Assistant General Counsel
       Shamai Elstein
       Counsel
       North American Electric Reliability Corporation
       1325 G St., NW, Suite 600
       Washington, DC 20005
       202-400-3000
       holly.hawkins@nerc.net
       shamai.elstein@nerc.net

---

[11] *Id*. at PP 181-184.

[12] *Id*. at P 209.

[13] *Id*. at P 210.

Attachment A

CIP-003-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. **Title:**   Cyber Security — Security Management Controls

2. **Number:**   CIP-003-5

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

4. **Applicability:**

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

  4.1.1 Balancing Authority

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

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

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

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

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

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

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

  4.1.3 Generator Operator

  4.1.4 Generator Owner

  4.1.5 Interchange Coordinator or Interchange Authority

  4.1.6 Reliability Coordinator

4.1.7   Transmission Operator

4.1.8   Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2   Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

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

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

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

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

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

5. **Effective Dates:**

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

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

6. **Background:**

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

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

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

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

are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

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

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

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

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

B. Requirements and Measures

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

    1.1   Personnel & training (CIP-004);

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

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

    1.4   System security management (CIP-007);

    1.5   Incident reporting and response planning (CIP-008);

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

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

    1.8   Information protection (CIP-011); and

    1.9   Declaring and responding to CIP Exceptional Circumstances.

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

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

    2.1   Cyber security awareness;

    2.2   Physical security controls;

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

    2.4   Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority:

   The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

   1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit

- Self-Certification

- Spot Checking

- Compliance Investigation

- Self-Reporting

- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

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

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
						previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2)

OR

The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as | The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2)

OR

The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as | The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2)

OR

The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. | The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2)

OR

The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)

OR |

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one	required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 17 calendar months but did complete this approval	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	in less than or equal to 18 calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document

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

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations

- Identification of possible disciplinary action for violating this policy

- Account management

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

- Organization stance on use of wireless networks

- Identification of acceptable authentication methods

- Identification of trusted and untrusted resources

- Monitoring and logging of ingress and egress at Electronic Access Points

- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access

- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access

- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access

- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

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

- Strategy for protecting Cyber Assets from unauthorized physical access

- Acceptable physical access control methods

- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening

- Acceptable methods of authentication and access control

- Password policies including length, complexity, enforcement, prevention of brute force attempts

- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident

- Obligations to report Cyber Security Incidents

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

- Availability of spare components

- Availability of system backups

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

- Initiation of change requests

- Approval of changes

- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods

- Notification of unauthorized information disclosure

- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance

- Processes to allow for exceptions to policy that do not violate CIP requirements

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

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

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

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

Requirement R4:

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

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

Rationale:

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

Rationale for R1:

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

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

Rationale for R2:

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

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

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

Rationale for R3:

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

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

Rationale for R4:

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

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5. (Order becomes effective 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify VSLs for Requirements R1 and R2.	

Redline

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-5

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

4. **Applicability:**

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

    4.1.1 Balancing Authority

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

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

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

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

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

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

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

    4.1.3 Generator Operator

    4.1.4 Generator Owner

    4.1.5 Interchange Coordinator or Interchange Authority

    4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

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

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

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

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

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

5. **Effective Dates:**

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

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

6. **Background:**

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

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

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

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

are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

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

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

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

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

B. Requirements and Measures

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

    1.1 Personnel & training (CIP-004);

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

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

    1.4 System security management (CIP-007);

    1.5 Incident reporting and response planning (CIP-008);

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

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

    1.8 Information protection (CIP-011); and

    1.9 Declaring and responding to CIP Exceptional Circumstances.

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

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

    2.1 Cyber security awareness;

    2.2 Physical security controls;

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

    2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit

- Self-Certification

- Spot Checking

- Compliance Investigation

- Self-Reporting

- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

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

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify,	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its	the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its	assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to~~	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	~~Requirement R2~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified

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

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations

- Identification of possible disciplinary action for violating this policy

- Account management

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

- Organization stance on use of wireless networks

- Identification of acceptable authentication methods

- Identification of trusted and untrusted resources

- Monitoring and logging of ingress and egress at Electronic Access Points

- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access

- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access

- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access

- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

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

- Strategy for protecting Cyber Assets from unauthorized physical access

- Acceptable physical access control methods

- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening

- Acceptable methods of authentication and access control

- Password policies including length, complexity, enforcement, prevention of brute force attempts

- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents

- Appropriate notifications upon discovery of an incident

- Obligations to report Cyber Security Incidents

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

- Availability of spare components

- Availability of system backups

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

- Initiation of change requests

- Approval of changes

- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods

- Notification of unauthorized information disclosure

- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance

- Processes to allow for exceptions to policy that do not violate CIP requirements

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

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

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

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

Requirement R4:

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

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

Rationale:

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

Rationale for R1:

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

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

Rationale for R2:

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

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

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

Rationale for R3:

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

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

Rationale for R4:

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

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

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5. (Order becomes effective 2/3/14.)	

CIP-004-5.1 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

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

2. **Number:**   CIP-004-5.1

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

4. **Applicability:**

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

   4.1.1.   Balancing Authority

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

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

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

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

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

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

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

   4.1.3.   Generator Operator

   4.1.4.   Generator Owner

   4.1.5.   Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

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

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

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

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

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. **Effective Dates:**

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

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

6. **Background:**

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

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

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

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

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

implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

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

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

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

B. Requirements and Measures

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

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

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

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

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

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures

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

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures

2.2	High Impact BES Cyber Systems and their associated:
	  1. EACMS; and
	  2. PACS
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	  1. EACMS; and
	  2. PACS
		Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

2.3	High Impact BES Cyber Systems and their associated:
	  1. EACMS; and
	  2. PACS
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	  1. EACMS; and
	  2. PACS
		Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

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

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

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

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures

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

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

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**

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

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

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

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**

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

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

CIP-004-5.1 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures

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

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**

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

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

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

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

	CIP-004-5.1 Table R5 – Access Revocation		
Part	**Applicable Systems**	**Requirements**	**Measures**

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

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

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

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit

- Self-Certification

- Spot Checking

- Compliance Investigation

- Self-Reporting

- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1)

OR

The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized | and correct the deficiencies. (2.1)

OR

The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2)

OR

The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized | and correct the deficiencies. (2.1)

OR

The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2)

OR

The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized | The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1)

OR

The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not |

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted	physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4)

OR

The Responsible Entity has implemented | physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)
OR

The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) | physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

OR

The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) | determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) |

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances, and did not identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

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

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

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);

- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3:

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

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include
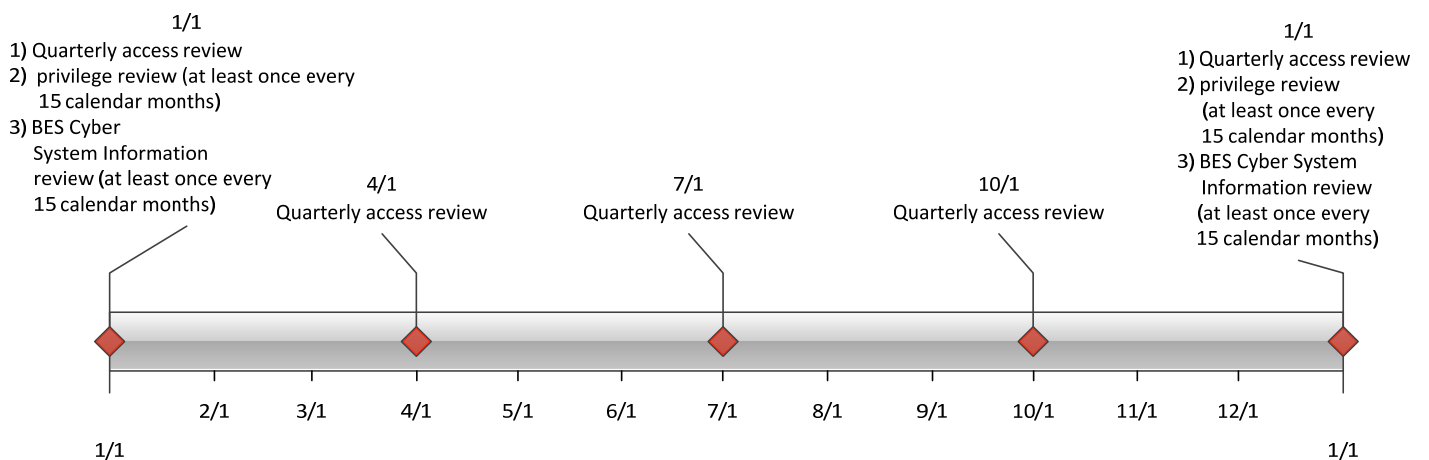
individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

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

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

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function

(i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

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

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

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

Requirement R5:

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

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

Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

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

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

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

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

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

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*

Moved example mechanisms to guidance.

Rationale for R2:

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

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:

- The visitor control program
- Electronic interconnectivity supporting the operation and control of BES Cyber Systems
- Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

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

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.   CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

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

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

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

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

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

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

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

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

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

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

*The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards **to require immediate revocation** for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Modified two VSLs in R4.	Errata
5.1	11/22/13	FERC Order issued approving CIP-004-5.1. (Order becomes effective on 2/3/14.)	

5.1	5/7/14	Adopted by the NERC Board of Trustees to modify the VRF and VSLs for Requirement R4.	

Redline

A. Introduction

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

2. **Number:**   CIP-004-5.1

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

4. **Applicability:**

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

    4.1.1. **Balancing Authority**

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

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

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

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

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

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

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

    4.1.3. **Generator Operator**

    4.1.4. **Generator Owner**

    4.1.5. **Interchange Coordinator or Interchange Authority**

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

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

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

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

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

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. **Effective Dates:**

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

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

6. **Background:**

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

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

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

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

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

implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

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

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

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

B. Requirements and Measures

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

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

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

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

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

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**

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

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

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

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

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

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

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures

3.3	High Impact BES Cyber Systems and their associated:
	   1. EACMS; and
	   2. PACS
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	   1. EACMS; and
	   2. PACS
		Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

3.4	High Impact BES Cyber Systems and their associated:
	   1. EACMS; and
	   2. PACS
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	   1. EACMS; and
	   2. PACS
		Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**

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

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

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

CIP-004-5.1 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures

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

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

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

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

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

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

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures

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

	CIP-004-5.1 Table R5 – Access Revocation		
Part	Applicable Systems	Requirements	Measures

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

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

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

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit

- Self-Certification

- Spot Checking

- Compliance Investigation

- Self-Reporting

- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	Operations Planning	Medium	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	Operations Planning and Same Day Operations	~~Lower~~Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2)

OR

The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 | The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for ~~two~~ more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3)

OR

The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System | The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for ~~three~~ more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3)

OR

The Responsible Entity has implemented processes to verify that access to the designated storage locations for | BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1)

OR

The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2)

OR

The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated |

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			calendar months of the previous verification but for ~~one~~ 5% or less of its BES Cyber System_s_, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its~~two~~ BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for ~~three~~ more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for ~~four or more~~more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for ~~four or more~~more than 15% of its BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Information is correct and necessary within 15 calendar months of the previous verification but for ~~one~~ 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more process(es) to	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted	physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances, and did not identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

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

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

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);

- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3:

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

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include
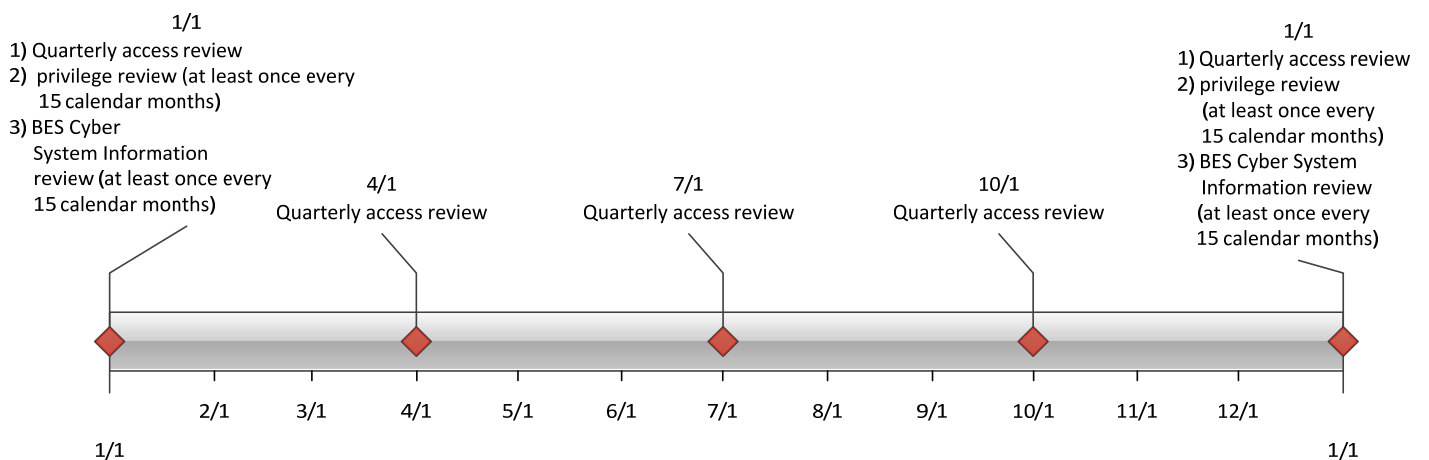
individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

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

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

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function

(i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

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

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

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

Requirement R5:

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

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

Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

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

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

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

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

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

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical access "received" ongoing reinforcement – to state that security awareness has been reinforced.

Moved example mechanisms to guidance.

Rationale for R2:

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

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:

- The visitor control program
- Electronic interconnectivity supporting the operation and control of BES Cyber Systems
- Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

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

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.   CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

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

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

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

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

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

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

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

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

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

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

*The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards **to require immediate revocation** for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Modified two VSLs in R4.	Errata
5.1	11/22/13	FERC Order issued approving CIP-004-5.1. (Order becomes effective on 2/3/14.)	

CIP-006-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1.   Title: Cyber Security — Physical Security of BES Cyber Systems

2.   Number: CIP-006-5

3.   Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4.   Applicability:

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

4.1.1   Balancing Authority

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

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

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

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

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

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

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

4.1.3   Generator Operator

4.1.4   Generator Owner

4.1.5   Interchange Coordinator or Interchange Authority

4.1.6   Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-5:

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

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

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

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

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

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

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

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.

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

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

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

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*.

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures

1.4	High Impact BES Cyber Systems and their associated:
	  1. EACMS; and
	  2. PCA
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	  1. EACMS; and
	  2. PCA
		Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

	CIP-006-5 Table R1– Physical Security Plan		
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.8	High Impact BES Cyber Systems and their associated: 　1. EACMS; and 　2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 　1. EACMS; and 　2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**

1.9	High Impact BES Cyber Systems and their associated:
	    1. EACMS; and
	    2. PCA
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	    1. EACMS; and
	    2. PCA
		Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures

2.1	High Impact BES Cyber Systems and their associated:
	  1. EACMS; and
	  2. PCA
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	  1. EACMS; and
	  2. PCA
		Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures

2.2	High Impact BES Cyber Systems and their associated:
	    1. EACMS; and
	    2. PCA
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	    1. EACMS; and
	    2. PCA
		Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

2.3	High Impact BES Cyber Systems and their associated:
	    1. EACMS; and
	    2. PCA
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	    1. EACMS; and
	    2. PCA
		Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

    1.1. Compliance Enforcement Authority:

    The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

    1.2. Evidence Retention:

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

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

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    1.3. Compliance Monitoring and Assessment Processes:

    - Compliance Audit

    - Self-Certification

    - Spot Checking

    - Compliance Investigation

    - Self-Reporting

    - Complaint

    1.4. Additional Compliance Information:

    - None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning Same-Day Operations	Medium	The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR The Responsible Entity	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8)

OR

The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified | identified deficiencies but did not assess or correct the deficiencies. (1.7)

OR

The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7) | has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5)

OR

The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5)

OR

The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the | assess, or correct the deficiencies. (1.1)

OR

The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2)

OR

The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or correct the deficiencies. (1.2)

OR

The Responsible Entity has documented and |

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)		deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)
						OR
						The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)
						OR
						The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter. (1.4)
						OR
						The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)
						OR
						The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4)
						OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Access Control Systems or to communicate such alerts within 15 minutes to identified personnel (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	Same-Day Operations	Medium	N/A	The Responsible Entity included a visitor control program that requires logging of each	The Responsible Entity included a visitor control program that requires continuous	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at	escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		
R3	Long Term Planning	Medium	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	did complete required testing within 26 calendar months. (3.1)	did complete required testing within 27 calendar months. (3.1)	has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.

- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.

- Video Recording: Electronic capture of video images of sufficient quality to determine identity.

- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.
FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).

Reference to prior version: (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-006-5. (Order becomes effective on 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify the VRF for Requirement R3.	

Redline

A. Introduction

1.   Title: Cyber Security — Physical Security of BES Cyber Systems

2.   Number: CIP-006-5

3.   Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4.   Applicability:

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

4.1.1   Balancing Authority

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

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

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

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

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

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

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

4.1.3   Generator Operator

4.1.4   Generator Owner

4.1.5   Interchange Coordinator or Interchange Authority

4.1.6   Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-5:

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

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

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

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

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

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

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

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.

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

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

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

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*.

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 　1.　EACMS; and 　2.　PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 　1.　EACMS; and 　2.　PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

	CIP-006-5 Table R1– Physical Security Plan		
Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures

2.2	High Impact BES Cyber Systems and their associated:
	    1. EACMS; and
	    2. PCA
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	    1. EACMS; and
	    2. PCA
		Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

2.3	High Impact BES Cyber Systems and their associated:
	    1. EACMS; and
	    2. PCA
	
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:
	    1. EACMS; and
	    2. PCA
		Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor:* ~~Lower~~*Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit

- Self-Certification

- Spot Checking

- Compliance Investigation

- Self-Reporting

- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long Term Planning Same-Day Operations	Medium	The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR The Responsible Entity	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified	identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the	assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)		deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter. (1.4)
						OR
						The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)
						OR
						The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4)
						OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Access Control Systems or to communicate such alerts within 15 minutes to identified personnel (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	Same-Day Operations	Medium	N/A	The Responsible Entity included a visitor control program that requires logging of each	The Responsible Entity included a visitor control program that requires continuous	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at	escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		
R3	**Long Term Planning**	~~Lower~~Medium	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	did complete required testing within 26 calendar months. (3.1)	did complete required testing within 27 calendar months. (3.1)	has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.

- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.

- Video Recording: Electronic capture of video images of sufficient quality to determine identity.

- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.
FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).

Reference to prior version: (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-006-5. (Order becomes effective on 2/3/14.)	

CIP-008-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-5

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

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

   4.1.1 Balancing Authority

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

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

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

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

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

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

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

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator or Interchange Authority

   4.1.6 Reliability Coordinator

   4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-5:

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

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

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

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. **Effective Dates:**

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. **Background:**

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

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

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

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

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

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

program could meet the requirements for training personnel across multiple BES Cyber Systems.

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment]*.

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**

3.1	High Impact BES Cyber Systems
	
	Medium Impact BES Cyber Systems
		No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:
		
		3.1.1. Document any lessons learned or document the absence of any lessons learned;
		
		3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and
		
		3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.
			An example of evidence may include, but is not limited to, all of the following:
			
			1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned;
			
			2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and
			
			3. Evidence of plan update distribution including, but not limited to:
			  • Emails;
			  • USPS or other mail service;
			  • Electronic distribution system; or
			  • Training sign-in sheets.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

    1.1. Compliance Enforcement Authority:

    The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

    1.2. Evidence Retention:

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

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

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    1.3. Compliance Monitoring and Assessment Processes:

    - Compliance Audit

    - Self-Certification

    - Spot Checking

    - Compliance Investigation

    - Self-Reporting

    - Complaint

    1.4. Additional Compliance Information:

    - None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
						not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with	The Responsible Entity has not updated the	The Responsible Entity has neither	The Responsible Entity has neither

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR	documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the	documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf

- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the

plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

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

4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5. (Order becomes effective on 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify the VSL for Requirement R2.	

Redline

A. Introduction

1. **Title:**   Cyber Security — Incident Reporting and Response Planning

2. **Number:**   CIP-008-5

3. **Purpose:**   To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

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

   4.1.1 **Balancing Authority**

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

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

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

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

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

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

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

   4.1.3 **Generator Operator**

   4.1.4 **Generator Owner**

   4.1.5 **Interchange Coordinator or Interchange Authority**

   4.1.6 **Reliability Coordinator**

   4.1.7 **Transmission Operator**

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-5:

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

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

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

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. **Effective Dates:**

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. **Background:**

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

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

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

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

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

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

program could meet the requirements for training personnel across multiple BES Cyber Systems.

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*.

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

    1.1. Compliance Enforcement Authority:

    The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

    1.2. Evidence Retention:

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

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

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    1.3. Compliance Monitoring and Assessment Processes:

    - Compliance Audit

    - Self-Certification

    - Spot Checking

    - Compliance Investigation

    - Self-Reporting

    - Complaint

    1.4. Additional Compliance Information:

    - None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	Operations Planning Real-time Operations	Lower	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within ~~19~~ 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with	The Responsible Entity has not updated the	The Responsible Entity has neither	The Responsible Entity has neither

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR	documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the	documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf

- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.
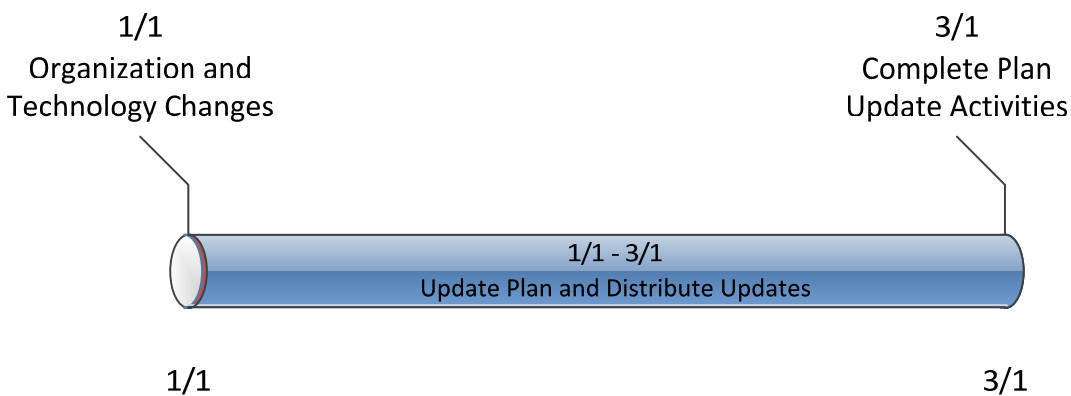

Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the

plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

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

4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5. (Order becomes effective on 2/3/14.)	

CIP-009-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-5

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. **Applicability:**

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

4.1.1 **Balancing Authority**

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

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

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

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

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

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

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

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 **Interchange Coordinator or Interchange Authority**

4.1.6 **Reliability Coordinator**

4.1.7   Transmission Operator

4.1.8   Transmission Owner

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

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

4.2.1.1   Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2   Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3   Exemptions: The following are exempt from Standard CIP-009-5:

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

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

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

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

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

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

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

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

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

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

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

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

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

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

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact BES Cyber Systems and their associated: 　1. EACMS; and 　2. PACS Medium Impact BES Cyber Systems and their associated: 　1. EACMS; and 　2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 　1. EACMS; and 　2. PACS Medium Impact BES Cyber Systems and their associated: 　1. EACMS; and 　2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures

2.2	High Impact BES Cyber Systems and their associated:
	    1. EACMS; and
	    2. PACS
	
	Medium Impact BES Cyber Systems at Control Centers and their associated:
	    1. EACMS; and
	    2. PACS
		Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.
		
		An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.
			An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

	CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication		
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures

3.2	High Impact BES Cyber Systems and their associated:
	   1. EACMS; and
	   2. PACS
	
	Medium Impact BES Cyber Systems at Control Centers and their associated:
	   1. EACMS; and
	   2. PACS
		No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:
		
		3.2.1. Update the recovery plan; and
		
		3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.
			An example of evidence may include, but is not limited to, all of the following:
			
			1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and
			
			2. Evidence of plan update distribution including, but not limited to:
			
			   • Emails;
			
			   • USPS or other mail service;
			
			   • Electronic distribution system; or
			
			   • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

    ### 1.1. Compliance Enforcement Authority:

    The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

    ### 1.2. Evidence Retention:

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

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

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    ### 1.3. Compliance Monitoring and Assessment Processes:

    - Compliance Audit

    - Self-Certification

    - Spot Checking

    - Compliance Investigation

    - Self-Reporting

    - Complaint

    ### 1.4. Additional Compliance Information:

    - None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R2	**Operations Planning** **Real-time Operations**	Lower	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR

The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)

OR

The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

OR

The Responsible Entity has tested the recovery plan(s) according to R2 Part |

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
						2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operation al%20Functions%20FINAL%20102511.pdf

- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;

2. Current backup tapes and any additional documented configuration settings;

3. Documented build or restoration procedures; and

4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.

- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.

- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.

- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1~~Figure 1~~, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2~~Figure 2~~, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.
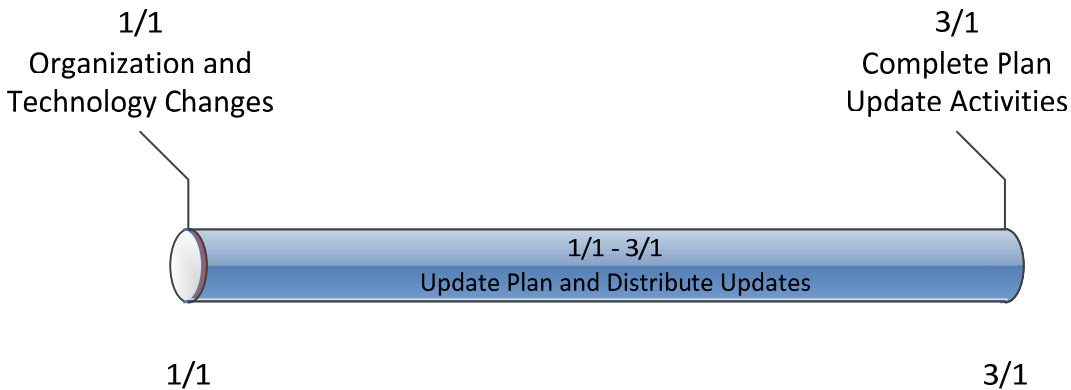
Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5. (Order becomes effective on 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify VSLs for Requirement R3.	

Redline

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-5

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. **Applicability:**

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

    4.1.1 Balancing Authority

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

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

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

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

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

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

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

    4.1.3 Generator Operator

    4.1.4 Generator Owner

    4.1.5 Interchange Coordinator or Interchange Authority

    4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-5:

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

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

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

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

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

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

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

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

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

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

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

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

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

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

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

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*.

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures

1.4	High Impact BES Cyber Systems and their associated:
	  1. EACMS; and
	  2. PACS
	
	Medium Impact BES Cyber Systems at Control Centers and their associated:
	  1. EACMS; and
	  2. PACS
		One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

1.5	High Impact BES Cyber Systems and their associated:
	  1. EACMS; and
	  2. PACS
	
	Medium Impact BES Cyber Systems and their associated:
	  1. EACMS; and
	  2. PACS
		One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.* *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 　1. EACMS; and 　2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 　1. EACMS; and 　2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures

2.2	High Impact BES Cyber Systems and their associated:
	   1. EACMS; and
	   2. PACS
	
	Medium Impact BES Cyber Systems at Control Centers and their associated:
	   1. EACMS; and
	   2. PACS
		Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.
		
		An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.
			An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

	CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication		
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures

3.2	High Impact BES Cyber Systems and their associated:
	   1. EACMS; and
	   2. PACS
	
	Medium Impact BES Cyber Systems at Control Centers and their associated:
	   1. EACMS; and
	   2. PACS
		No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:
		
		3.2.1. Update the recovery plan; and
		
		3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.
			An example of evidence may include, but is not limited to, all of the following:
			
			1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and
			
			2. Evidence of plan update distribution including, but not limited to:
			
			   • Emails;
			
			   • USPS or other mail service;
			
			   • Electronic distribution system; or
			
			   • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

    ### 1.1. Compliance Enforcement Authority:

    The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

    ### 1.2. Evidence Retention:

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

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

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    ### 1.3. Compliance Monitoring and Assessment Processes:

    - Compliance Audit

    - Self-Certification

    - Spot Checking

    - Compliance Investigation

    - Self-Reporting

    - Complaint

    ### 1.4. Additional Compliance Information:

    - None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R2	**Operations Planning** **Real-time Operations**	Lower	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than ~~210~~ 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

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

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

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

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf

- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;

2. Current backup tapes and any additional documented configuration settings;

3. Documented build or restoration procedures; and

4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.

- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.

- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.

- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1~~Figure 1~~, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.
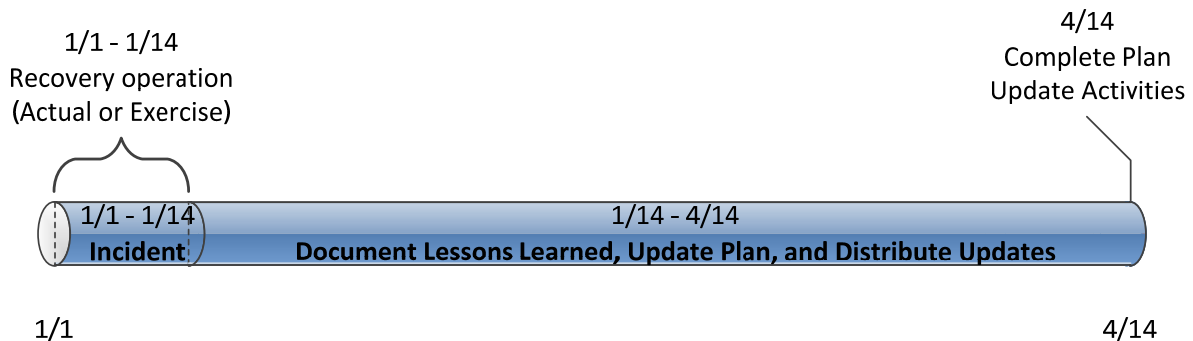

Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2~~Figure 2~~, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.
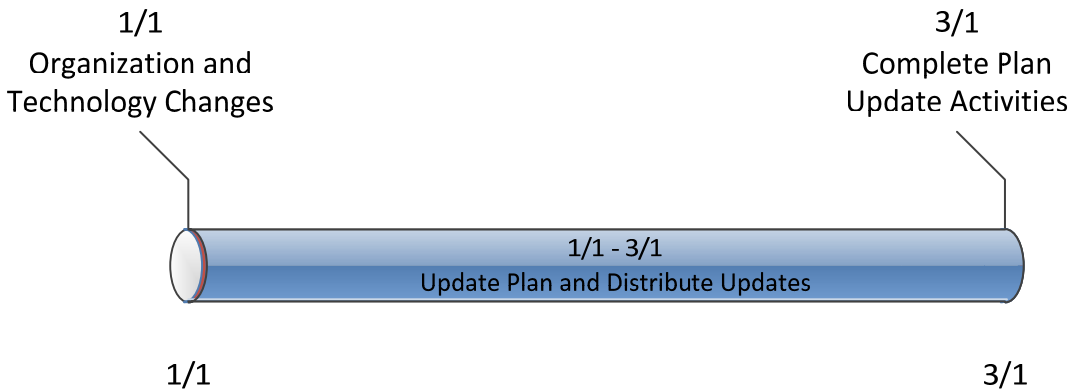
1/1
Organization and
Technology Changes

3/1
Complete Plan
Update Activities

1/1 - 3/1
Update Plan and Distribute Updates

1/1

3/1

Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

 Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

 Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5. (Order becomes effective on 2/3/14.)	